

CERTIFICATES OF POSITIVITY IN THE BERNSTEIN BASIS

FATIMA BOUDAUD FABRIZIO CARUSO MARIE-FRANÇOISE ROY

novembre 3, 2006

ABSTRACT. Let $P \in \mathbb{Z}[X]$ be a polynomial of degree p with coefficients 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 .

1. INTRODUCTION: CERTIFICATES OF POSITIVITY

Throughout the paper we are using the Bernstein polynomials, in order to obtain certificates of positivity, i.e. algebraic identities certifying the positivity of a given polynomial on an interval. We denote by R a real closed field, and consider polynomials in $R[X]$.

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

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

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

Note that

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

Given a list b with $p+1$ elements, we denote its elements by $b_i, i = 0, \dots, p$, and $b \in \mathbb{Z}^{p+1}$ means $\forall i \in \{0, \dots, p\} b_i \in \mathbb{Z}$. If P is a polynomial of degree $\leq p$, we denote by $b(P, p, \ell, r)$ 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 . Note also that $b(1, p, \ell, r) = [1, \dots, 1]$.

It is useful to recall the very simple Algorithm by which $b(P, p, \ell, m)$ and $b(P, p, m, r)$ are computed from $b(P, p, \ell, r)$ [1].

Algorithm 1.

- **Input:** $b = b(P, p, \ell, r), m$.
- **Output:** $b' = b(P, p, \ell, m), b'' = b(P, p, m, r)$.
- **Procedure:**
 - Initialization: $b_j^{(0)} := b_j$, for $j = 0, \dots, p$.
 - $\alpha := (r - m)/(r - \ell)$.
 - For $i = 1, \dots, p$,
 - For $j = 0, \dots, p - i$, compute
$$b_j^{(i)} := \alpha b_j^{(i-1)} + (1 - \alpha) b_{j+1}^{(i-1)}.$$
 - Output
$$b' = b_0^{(0)}, \dots, b_0^{(j)}, \dots, b_0^{(p)},$$

$$b'' = b_0^{(p)}, \dots, b_j^{(p-j)}, \dots, b_p^{(0)}.$$

Let us define $\mathbf{Cert}(b)$, where b is a list of elements of R by: **all the elements of b are non negative, with $b_0 > 0$, $b_d > 0$** . $\mathbf{Cert}(b(P, d, \ell, r))$ means that the expression of P in the Bernstein basis of degree d for ℓ, r provides a certificate of positivity for P on $[\ell, r]$, i.e. a description of P making obvious that it is positive on $[\ell, r]$. We also define $\mathbf{Cert}^*(b)$: **all the elements of b are positive**.

Remark 1. a) If $\mathbf{Cert}(b(P, d, \ell, r))$, it follows from Algorithm 2 that $\mathbf{Cert}^*(b(P, d, \ell, m))$ and $\mathbf{Cert}^*(b(P, d, m, r))$ hold for every m such that $\ell < m < r$.

b) If $\mathbf{Cert}(b(P_1, d_1, \ell, r))$ and $\mathbf{Cert}(b(P_2, d_2, \ell, r))$, $\mathbf{Cert}(b(P_1 P_2, d_1 + d_2, \ell, r))$. This follows immediately from the multiplication law in the Bernstein basis:

$$\text{Bern}_{d_1, i_1}(\ell, r) \text{Bern}_{d_2, i_2}(\ell, r) = \left(\left(\binom{d_1}{i_1} \binom{d_2}{i_2} \right) / \binom{d_1 + d_2}{i_1 + i_2} \right) \text{Bern}_{d_1 + d_2, i_1 + i_2}(\ell, r).$$

c) If $\mathbf{Cert}(b(P, d, \ell, r))$ (resp. $\mathbf{Cert}^*(b(P, d, \ell, r))$) and $d' \geq d$, then $\mathbf{Cert}(b(P, d', \ell, r))$ (resp. $\mathbf{Cert}^*(b(P, d', \ell, r))$): apply b) to $P_1 = P, P_2 = 1, d_1 = d, d_2 = d' - d$.

d) If $\mathbf{Cert}(b(P, d, \ell, r))$, then $\mathbf{Cert}^*(b(P, 2d, \ell, r))$: multiply P and 1 expressed in the Bernstein basis of degree d for ℓ, r , using the multiplication law in the Bernstein basis. \square

If P is of degree p and $\mathbf{Cert}(b(P, p, -1, 1))$ holds, 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 $\mathbf{Cert}(b(P, p, -1, 1))$ does not hold. Consider for example the polynomial

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

It is immediate to check that P is positive on $[-1, 1]$, but $b(P, 2, -1, 1) = [10, -4, 2]$ and $\mathbf{Cert}(b(P, 2, -1, 1))$ does not hold. However, since

$$b(P, 21, -1, 1) = [210, 182, 156, 132, 110, 90, 72, 56, 42, 30, 20, 12, 6, 2, 0, 0, 2, 6, 12, 20, 30, 42], \quad (2)$$

$\mathbf{Cert}(b(P, 21, -1, 1))$. Moreover 21 is the smallest natural number with this property.

Bernstein proved the following result [3]: if a non zero univariate polynomial $P \in \mathbb{R}[X]$ of degree p is positive on $[-1, 1]$, there exists $d \geq p$ such that $\mathbf{Cert}^*(b(P, d, -1, 1))$. In other words, by increasing the degree of the Bernstein basis, a positive polynomial on $[-1, 1]$ gets a certificate of positivity. The smallest natural number d such that $\mathbf{Cert}^*(b(P, d, -1, 1))$ is called the **Bernstein degree** of P .

Note that if $P \in R[X]$ where R is a general real closed field, there does not necessary exists d such that $\mathbf{Cert}^*(b(P, d, -1, 1))$.

Example 2. Let R be non archimedean and ε an element of R which is infinitesimal i.e. positive and smaller than any positive rational number. The polynomial $P = (1 - \varepsilon) X^2 + \varepsilon$ is positive on $[-1, 1]$ but for every $d \in \mathbb{N}$, $\mathbf{Cert}(b(P, d, -1, 1))$ does not hold. Thus, it follows from Remark 1 c) that for every $d \in \mathbb{N}$, $\mathbf{Cert}^*(b(P, d, -1, 1))$ does not hold either.

Indeed, we have $b(P, 2, -1, 1) = [1, 2\varepsilon - 1, 1]$, thus for any $d \geq 2$

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

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

$$\binom{d}{n} b(P, d, -1, 1)_n = \binom{d-2}{n-2} + \binom{d-2}{n-1} (4\varepsilon - 2) + \binom{d-2}{n}, \quad (3)$$

– If d is even, take $n = d/2$, it follows from (3) that

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

– If d is odd, take $n = (d - 1)/2$, it follows from (3) that

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

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

Remark 3. Bernstein's result (2) is equivalent to a famous result of Polya stating that a non zero polynomial P is strictly positive on $(0, +\infty)$ if and only if there exists n such that $(1 + X)^n P$ has positive coefficients, which is a certificate of positivity of P on $(0, +\infty)$. The **Polya degree** is the smallest natural number such that this property holds. The equivalence between the two results is immediate using the Goursat transform sending a polynomial P of degree p to

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

since in the Goursat transformation monomials X^i are sent to $(1 - X)^i (1 + X)^{p-i}$. \square

In 2001, Powers and Reznick proved in [7] a quantitative bound on the Bernstein degree, estimating it by

$$\frac{p(p-1)}{2} \frac{M}{\lambda} \quad (4)$$

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 [7] needs to be corrected as in (3) [8]. We shall see later in the paper that such a bound is exponential in p and τ , and that the corresponding certificate of positivity can indeed be exponentially large in some special cases.

Here we obtain a different kind certificate of positivity for P on $[-1, 1]$ using also the Bernstein basis. Our point of view is that it is better to keep the initial degree, and to refine the interval, looking for certificates of positivity on subintervals. A **subdivision L of $[-1, 1]$ of length n** is an ordered list $\ell_0 = -1 < \ell_1 < \dots < \ell_n < \ell_{n+1} = 1$. The subdivision L is **rational** if all ℓ_i are rational numbers. Property **Cert**($b(P, p, L)$) is defined as: **for every $i = 1 \dots n + 1$, Cert**($b(P, p, \ell_{i-1}, \ell_i)$). Let $c = (c_1, \dots, c_n) \in (\mathbb{N}^*)^n$. Property **Cert $_{\mathbb{Z}}$** ($b(cP, p, L)$) is defined as: **for every $i = 1 \dots n + 1$, Cert**($b(c_i P, p, \ell_{i-1}, \ell_i)$) and $b(c_i P, p, \ell_{i-1}, \ell_i) \in \mathbb{Z}^{p+1}$. We denote by $b(cP, p, L)$ the list of $[\ell_{i-1}, \ell_i], c_i, b(c_i P, p, \ell_{i-1}, \ell_i), i = 1, \dots, n$. Our main results in the paper are

- the existence, in any real closed field R , of a subdivision L of length at most p such that $\text{Cert}(b(P, p, L))$,
- the fact that, if $P \in \mathbb{Z}[X]$ it is possible to chose L rational and $c \in (\mathbb{N}^*)^{n+1}$ such that the $\text{Cert}_{\mathbb{Z}}(b(cP, p, L))$ and the bit-size of $b(cP, p, L)$ is at most $O(p^4(\tau + \log_2 p))$, i.e. polynomial in p and τ .

The reason why $b(cP, p, L)$ is shorter than $b(P, d, -1, 1)$ where d is the Bernstein degree 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 adaptativity is the key to the exponential gain given by our certificate.

In our example $P = 5X^2 - 4X + 1$, we obtain that $\text{Cert}_{\mathbb{Z}}(b(cP, p, L))$, with $L = -1, 0, 1/2, 1$, $c = (1, 4, 4)$:

$$b(cP, p, L) = [[-1, 0], 1, [10, 3, 1]], [[0, 1/2], 4, [4, 0, 1]], [[1/2, 1], 4, [1, 2, 8]]$$

which reads as

- $b(P, 2, -1, 0) = [10, 3, 1]$,
- $b(4P, 2, 0, 1/2) = [4, 0, 1]$,
- $b(4P, 2, 1/2, 1) = [1, 2, 8]$.

It is clear that $b(cP, 2, L)$ is shorter than $b(P, 21, -1, 1)$ obtained in (2).

Let us prove now that there exists L such that $\text{Cert}(b(P, p, L))$ is true in a general real closed field R .

We denote by $\text{Var}(a)$ the number of sign variations in a sequence, $a = a_0, \dots, a_p$, of elements in $R \setminus \{0\}$, i.e. the number defined by induction on p by:

$$\begin{aligned} \text{Var}(a_0) &= 0 \\ \text{Var}(a_0, \dots, a_p) &= \begin{cases} \text{Var}(a_1, \dots, a_p) + 1 & \text{if } a_0 a_1 < 0 \\ \text{Var}(a_1, \dots, a_p) & \text{if } a_0 a_1 > 0 \end{cases} \end{aligned}$$

This definition extends to any finite sequence a of elements in R by considering the finite sequence b obtained by dropping the zeros in a and defining

$$\text{Var}(a) = \text{Var}(b), \text{Var}(\emptyset) = 0.$$

The following holds [1]:

Proposition 4. *Let P be of degree $\leq p$. Let $\text{num}(P; (\ell, r))$ be the number of roots of P in (ℓ, r) counted with multiplicities. Then*

- $\text{Var}(b(P, p, \ell, r)) \geq \text{num}(P; (\ell, r))$,
- $\text{Var}(b(P, p, \ell, r)) - \text{num}(P; (\ell, r))$ is even.

A partial reciprocal is true. Denote by $\mathcal{C}(\ell, r)$ the closed disk with $[\ell, r]$ as a diameter, by $C_1(\ell, r)$ the closed disk whose boundary circumscribes the equilateral triangle T_1 based on $[\ell, r]$ and by $C_2(\ell, r)$ the closed disk symmetric to $C_1(\ell, r)$ with respect to the X -axis (see Figure 1).

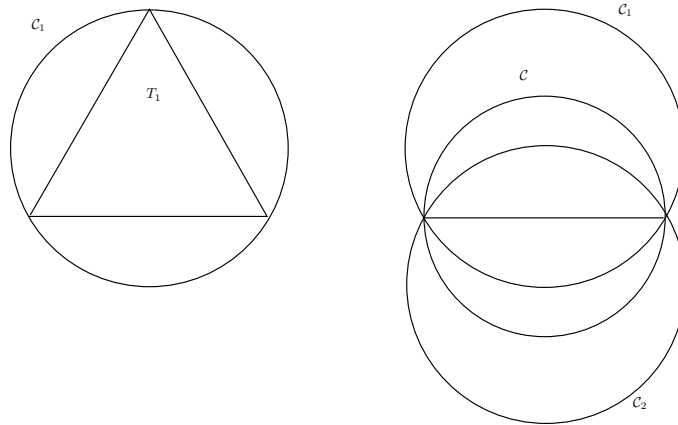


Figure 1. $C_1(\ell, r)$, then $\mathcal{C}(\ell, r)$, $C_1(\ell, r)$ and $C_2(\ell, r)$

Theorem 5. [Theorem of three circles]

Let $P \in R[X]$ be a square free polynomial of degree p .

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

b) If P has exactly one root in $C_1(\ell, r) \cup C_2(\ell, r)$, then $\text{Var}(b(P, p, \ell, r)) = 1$.

Theorem 6.

If $P \in R[X]$ be positive on $[-1, 1]$, there exists a subdivision L of $[-1, 1]$, of length at most p such that $\text{Cert}(b(P, p, L))$.

Proof: If P is square free, let $y_1 < \dots < y_r$, $2r \leq p$, be the elements of $[-1, 1]$ which are the projections of a set of roots Z_j , $j = 1, \dots, r$ of P in $C = R[i]$.

If $y_1 \neq -1$ and $y_r \neq 1$, let $\delta > 0$ be smaller than $(y_1 + 1)$, $(1 - y_r)$, $\min_{j=1 \dots r, z \in Z_j} |z - y_j|$ and $\min_{j=1 \dots r-1} (y_{j+1} - y_j)$. Define $n = 2r$, $\ell_0 = -1$, $\ell_{2j-1} = y_j - \delta$, $\ell_{2j} = y_j + \delta$, $j = 1, \dots, r$, $\ell_{2r+1} = 1$. Since, for $i = 1, \dots, n$, P has no root in $\mathcal{C}(\ell_{i-1}, \ell_i)$, Theorem 5 b) implies $\text{Cert}(b(P, p, \ell_{i-1}, \ell_i))$.

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

When P is not square free, let $P = P_1^2 \dots P_k^k$ be a square free decomposition of P given by non constant, pairwise coprime, polynomials P_1, \dots, P_k . Suppose without loss of generality that $\text{Cert}(b(P_i, p, L_i))$ for every $i = 1, \dots, k$ and let L be the ordered list given by the union of the L_i . The fact that $\text{Cert}(b(P, p, L))$ follows from Remark 1. \square

Remark 7. If F is an ordered field, R its real closure and $P \in F[X]$, the statement of Theorem 6 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 $\mathbb{R}(\varepsilon)$ its real closure, i.e. the field of algebraic Puiseux series with coefficients in \mathbb{R} . Take $P = X^4 + 2\varepsilon^2 X^2 - 2\varepsilon X^2 + \varepsilon^4 + 2\varepsilon^3 + \varepsilon^2$, whose roots are $\pm\sqrt{\varepsilon} \pm i\varepsilon$. Since, for ℓ, r in $\mathbb{R}(\varepsilon)$ with $-1 \leq \ell < \sqrt{\varepsilon} < r \leq 1$, denoting by $\bar{\ell}, \bar{r}$ the real numbers infinitely close to ℓ, r , and noting that $\bar{\ell} \leq 0, \bar{r} > 0$, one can compute that

$$\begin{aligned} b(P, 4, \ell, r) &= [\varepsilon^2 + \dots, ?, -\frac{4\varepsilon}{3}\bar{r}^2 + \dots, -\varepsilon\bar{r}^2 + \dots, \bar{r}^4 + \dots], \text{ if } \bar{\ell} = 0, \\ b(P, 4, \ell, r) &= [\bar{\ell}^4 + \dots, \bar{\ell}^3 r + \dots, \bar{\ell}^2 r^2 + \dots, \bar{\ell} r^3 + \dots, \bar{r}^4 + \dots], \text{ if } \bar{\ell} \neq 0 \end{aligned}$$

where $+\dots$ stands for “terms of higher order in ε ”, and $?$ for a quantity whose sign is not determined. It is easy to check that $\text{Var}(b(P, \ell, r)) > 0$ in all cases. \square

Remark 8. It is always possible to get a short certificate from a long one. If there exists a subdivision L of length N such that $\text{Cert}(b(P, p, L))$, there exists a subdivision L' contained in L of length at most p such that $\text{Cert}(b(P, p, L'))$. The subdivision L' can be extracted from L as follows: put in L' the extremities of the intervals $[\ell_{i-1}, \ell_i]$ in L such that there exists a root z of P with real part in $[\ell_{i-1}, \ell_i]$. Theorem 5 b) implies $\text{Cert}(b(P, p, L'))$ \square

The main purpose of the end of the paper is to give an algorithm constructing L and c such that $\text{Cert}_{\mathbb{Z}}(b(cP, p, L))$ whose size is polynomials in p and τ . In Section 2, we refine slightly the complexity results of [1] for real root isolation. In Section 3 we study the square free case, and consider the general case in Section 4. In Section 5 we compare in theory and in practice our certificate with the one obtained by Bernstein theorem and prove that our result provides an improvement from exponential to polynomial size. All the algorithms appearing in the paper have been implemented in SARAG [5].

2. COMPLEXITY OF REAL ROOT ISOLATION

This section is of expository nature. We extend slightly some recent results in [1]. This extension will be useful in Section 4 to prove the bound on our certificate of positivity.

2.1. Bounds on roots of a univariate polynomials.

We are going to use the following notions. Let

$$P = a_p X^p + \dots + a_0 \in \mathbb{C}[X], a_p \neq 0,$$

The **norm** of P is

$$\|P\| = \sqrt{|a_p|^2 + \dots + |a_0|^2}.$$

The **length** of P is

$$\text{Len}(P) = |a_p| + \dots + |a_0|.$$

Let z_1, \dots, z_p be the roots of P in \mathbb{C} counted with multiplicity so that

$$P = a_p \prod_{i=1}^p (X - z_i). \tag{5}$$

The **measure** of P is

$$\text{Mea}(P) = |a_p| \prod_{i=1}^p \max(1, |z_i|).$$

These quantities are related as follows [1]

$$\begin{aligned} \text{Len}(P) &\leq 2^p \text{Mea}(P) \\ \text{Mea}(P) &\leq \|P\| \end{aligned}$$

As a consequence, using the obvious fact that

$$\text{Mea}(Q) \leq \text{Mea}(P),$$

we deduce

Proposition 9. *If $P \in \mathbb{Z}[X]$ and $Q \in \mathbb{Z}[X]$, $\deg(Q) = q$, Q divides P , then*

$$\text{Len}(Q) \leq 2^q \|P\|.$$

and its corollary

Corollary 10. *If $P \in \mathbb{Z}[X]$ and $Q \in \mathbb{Z}[X]$ divides P in $\mathbb{Z}[X]$, then the bit-size of any coefficient of Q in the monomial basis is bounded by $q + \tau + \nu$, where τ is a bound on the bit-sizes of the coefficients of P in the monomial basis and ν is the bit-size of $p + 1$.*

Our next result is a mathematical statement expressing that the product of the distances between the roots of a polynomial cannot be arbitrarily small [6, 1].

We recall the classical definition of discriminant (see [1] for example). Let $P \in \mathbb{R}[X]$ be a polynomial of degree p ,

$$P = a_p X^p + a_{p-1} X^{p-1} + \dots + a_0,$$

and let x_1, \dots, x_p be the roots of P in \mathbb{C} (repeated according to their multiplicities). The **discriminant** of P , $\text{Disc}(P)$, is defined by

$$\text{Disc}(P) = a_p^{2p-2} \prod_{p \geq i > j \geq 1} (x_i - x_j)^2.$$

If $P \in \mathbb{Z}[X]$, $\text{Disc}(P) \in \mathbb{Z}$.

Proposition 11. *Let $Z = \text{Zer}(P, \mathbb{C})$ and $G = (Z, E)$ a directed acyclic graph such that*

- a) *for all $(z_i, z_j) \in E$, $|z_i| \leq |z_j|$,*
- b) *the in-degree of G is at most 1, i.e. for every $z_j \in Z$, there is at most one element z_i of Z such that $(z_i, z_j) \in E$.*

Then, denoting by m the number of elements of E ,

$$\prod_{(z_i, z_j) \in E} |z_i - z_j| \geq (p/\sqrt{3})^{-m} p^{-p/2} |\text{Disc}(P)|^{1/2} \text{Mea}(P)^{1-p}.$$

The following proposition is a slight variant of Proposition 11, useful to study the complexity of computing our certificate of positivity in Section 4.

Proposition 12. *Let P be of degree at most p with coefficients in \mathbb{Z} of bit-size bounded by τ and Q a square free divisor of P . Let $Z = \text{Zer}(Q, \mathbb{C})$ and $G = (Z, E)$ a directed acyclic graph such that*

- a) *for all $(z_i, z_j) \in E$, $|z_i| \leq |z_j|$,*
- b) *the in-degree of G is at most 1.*

Then, denoting by m the number of elements of E ,

$$\prod_{(z_i, z_j) \in E} |z_i - z_j| \geq (q/\sqrt{3})^{-m} q^{-q/2} (p+1)^{(1-q)/2} 2^{\tau(1-q)}.$$

Proof: Since $\text{Mea}(Q) \leq \text{Mea}(P)$, the claim follows from Proposition 11 for Q and $|\text{Disc}(Q)| \geq 1$, since it is clear that $\text{Mea}(P) \leq \|P\| \leq (p+1)^{1/2} 2^\tau$. \square

2.2. Real root isolation.

We give a variant of the Real Root Isolation Algorithm isolating roots on $[-1, 1]$. Let Z be a finite subset of \mathbb{R} . An **isolating list for Z** is a finite list L of rational points and open intervals with rational end points of \mathbb{R} , such that each element of L contains exactly one element of Z , every element of Z belongs to an element of L and two elements of L have an empty intersection.

We now indicate useful relationships between the basis of monomials and the Bernstein basis. We need the following notation.

- **Reciprocal polynomial in degree p :**

$$\text{Rec}_p(P(X)) = X^p P(1/X).$$

The non-zero roots of P are the inverses of the non-zero roots of $\text{Rec}(P)$.

- **Contraction by ratio λ :** for every non-zero λ ,

$$\text{Co}_\lambda(P(X)) = P(\lambda X).$$

The roots of $\text{Co}_\lambda(P)$ are of the form x/λ , where x is a root of P .

- **Translation by c :** for every c ,

$$\text{T}_c(P(X)) = P(X - c).$$

The roots of $\text{T}_c(P(X))$ are of the form $x + c$ where x is a root of P .

Proposition 13. *Let $P = \sum_{i=0}^p b_i \text{Bern}_{p,i}(\ell, r) \in \mathbb{R}[X]$ be of degree $\leq p$. Let*

$$\text{T}_{-1}(\text{Rec}_p(\text{Co}_{r-\ell}(\text{T}_{-\ell}(P)))) = \sum_{i=0}^p c_i X^i.$$

Then $\binom{p}{i} b_i = c_{p-i}$.

Proof: Performing the contraction of ratio $r - \ell$ after translating by $-\ell$ transforms $\binom{p}{i} (r - X)^{p-i} (X - \ell)^i / (r - \ell)^p$ into $\binom{p}{i} (1 - X)^{p-i} X^i$. Translating by -1 after taking the reciprocal polynomial in degree p transforms $\binom{p}{i} (1 - X)^{p-i} X^i$ into $\binom{p}{i} X^{p-i}$. \square

Corollary 14. *Let $P \in \mathbb{Z}[X]$ be of degree $\leq p$. If the bit-sizes of the coefficients of P are bounded by τ in the monomial basis $1, X, \dots, X^{p-1}$, then there exists $c \in \mathbb{Z}$ such that $b(cP, p, -1, 1) \in \mathbb{Z}^{p+1}$ and the bit-sizes of the $b(cP, p, -1, 1)_i$ are bounded by $p\nu + p + \tau + \nu$.*

Proof: If $P = \sum_{i=0}^p a_i X^i$, then it is easy to check that

$$Q = \text{T}_{-1}(\text{Rec}_p(\text{Co}_2(\text{T}_{-1}(P)))) = \sum_{i=0}^p a_i (X - 1)^{p-i} (X + 1)^i X^i \in \mathbb{Z}[X] \quad (6)$$

Defining c_i by $Q = \sum_{i=0}^p c_i X^i$,

$$b(P, p, -1, 1)_i = c_{p-i} / \binom{p}{i} \quad (7)$$

by Proposition 13. For every i , $\binom{p}{i}$ divides $p!$, thus $b(p!P, p, -1, 1) \in \mathbb{Z}^{p+1}$. Since the bit-size of $p!$ is at most $p\nu$, the conclusion on the bit-size of $b(p!P, p, -1, 1)_i$ follows easily from (7) since the bit-size of c_i is at most $p + \tau + \nu$ by (6). \square

Remark 15. In practice, the smallest value of c such that $b(cP, p, -1, 1) \in \mathbb{Z}^{p+1}$ is a divisor of $p!$ and is much smaller than $p!$. \square

In order to avoid denominators it is useful to make more precise Algorithm 1 [1].

Algorithm 2.

- **Input:** $([\ell, r], c, b(cP, p, \ell, r))$ and m , such that $b(cP, p, \ell, r) \in \mathbb{Z}^{p+1}$, $c \in \mathbb{N}$, and ℓ, m, r are in \mathbb{Q} .
- **Output:** $([\ell, m], c', b(c'P, p, \ell, m))$ and $([m, r], c', b(c'P, p, m, r))$, such that $b(c'P, p, \ell, m) \in \mathbb{Z}^{p+1}$, $c' \in \mathbb{N}$, $b(c'P, p, m, r) \in \mathbb{Z}^{p+1}$.
- **Procedure:**
 - Initialization: $b_j^{(0)} := b(cP, p, \ell, r)_j$, for $j = 0, \dots, p$.

- Let D be the lcm of the denominators of ℓ, m, r and $\ell' := D\ell, m' := Dm, r' := Dr$.
- For $i = 1, \dots, p$,
 - For $j = 0, \dots, p - i$, compute

$$b_j^{(i)} := (r' - m') b_j^{(i-1)} + (m' - \ell') b_{j+1}^{(i-1)}.$$
 - Output

$$\begin{aligned} b(c'P, p, \ell, m) &= (r' - \ell')^p b_0^{(0)}, \dots, (r' - \ell')^{p-j} b_0^{(j)}, \dots, b_0^{(p)}, \\ b(c'P, p, m, r) &= b_0^{(p)}, \dots, (r' - \ell')^{p-j} b_j^{(p-j)}, \dots, (r' - \ell')^p b_p^{(0)}, \\ c' &= (r' - m')^p c \end{aligned}$$

The following result follows immediately from Corollary 14 and Algorithm 2, computing $b(cP, p, \ell, r) \in \mathbb{Z}^{p+1}$ from $b(aP, p, -1, 1) \in \mathbb{Z}^{p+1}$ by two calls of Algorithm 2 first with input $b(aP, p, -1, 1)$ and ℓ , and output $b(a'P, p, \ell, 1)$ then with input $b(a'P, p, \ell, 1)$ and r .

Corollary 16. *Let $P \in \mathbb{Z}[X]$ be of degree $\leq p$. If the bit-sizes of the coefficients of P are bounded by τ in the monomial basis $1, X, \dots, X^{p-1}$, and ℓ and r are rational numbers of the form $\ell'/2^{\tau'}$, $m'/2^{\tau'}$ with ℓ', m' integers of bit-size bounded by τ' , then there exists $c \in \mathbb{Z}$ such that $b(cP, p, \ell, r) \in \mathbb{Z}^{p+1}$ and the bit-sizes of the $b(cP, p, -1, 1)_i$ are bounded by $p\nu + p + \tau + \nu + 2p\tau'$.*

We can now give our variant of real root isolation.

Algorithm 3.

- **Input:** a non-zero square free polynomial $P \in \mathbb{Z}[X]$ of degree p .
- **Output:** a list of rational numbers L isolating for the zeroes of P in $(-1, 1)$.
- **Procedure:**
 - Compute $c \in \mathbb{N} \setminus \{0\}$ such that $b(cP, p, -1, 1) \in \mathbb{Z}^{p+1}$ using (7) (and Remark 15).
 - Initialization: $M := \{((-1, 1), c, b(cP, p, -1, 1))\}$, $L := \emptyset$.
 - While Pos is non-empty,
 - Remove an element $((\ell, r), c, b(cP, p, \ell, r))$ from M .
 - If $\text{Var}(b(cP, p, \ell, r)) = 1$, add (ℓ, r) to L .
 - If $\text{Var}(b(cP, p, \ell, r)) > 1$, let $m = (\ell + r)/2$
 - compute b' and b'' , using Algorithm 2 with input $b(cP, p, \ell, r)$ and add

$$((\ell, m), 2^p c, b(2^p cP, p, \ell, m)), ((m, r), 2^p c, b(2^p cP, p, m, r))$$
 to M .
 - If $\text{sign}(b(2^p cP, p, \ell, m)_p) = 0$, add $\{m\}$ to L .

The correctness and termination of Algorithm 3 are similar to the proofs found in [1].

In terms of complexity, the following proposition is crucial. Let p be the degree of P , ν the bit-size of $p + 1$, τ a bound on the bit-size of the coefficients of P , and $Q \in \mathbb{Z}[X]$ a divisor of P

Proposition 17. *The number of applications of Algorithm 2 in Algorithm 3 applied to Q is at most $2(2\tau + 3\nu + 3)q$.*

Proof: The proof is similar to the proof of Proposition 10.50 in [1], using Proposition 12 rather than Corollary 10.24 in the proof. \square

Remark 18. Since the bit-size of the coefficients of Q are estimated by $O(\tau + p)$, a direct application of Proposition 10.50 of [1] would give $O((\tau + p)q)$. This is the reason why Proposition 12 is useful. \square

3. CERTIFICATE OF POSITIVITY IN THE SQUARE FREE CASE

In this section we consider a square free polynomial P and construct

- a certificate of positivity if the polynomial is positive on $[-1, 1]$,
- a point x of $[-1, 1]$ such that $Q(x) \leq 0$ otherwise.

Let us explain the mechanism of the algorithm. We try to isolate the real roots of P using Algorithm 3, and if we do not succeed, we notice that we produced a certificate that the polynomial is positive (or negative). The certificate of positivity (or negativity) obtained this way can then be compressed using Remark 8.

Algorithm 4. [Square free certificate of positivity]

- **Input:** a non-zero square-free polynomial $P \in \mathbb{Z}[X]$ of degree p .
- **Output:**
 - POS if $P > 0$ on $[-1, 1]$, with a rational subdivision L of $[-1, 1]$ of length $n \leq p$, and $c \in (\mathbb{N}^*)^{n+1}$ such that $\text{Cert}_{\mathbb{Z}}(b(cP, p, L))$.
 - NEG if $P < 0$ on $[-1, 1]$, with a rational subdivision L of $[-1, 1]$ of length $n \leq p$, and $c \in (\mathbb{N}^*)^{n+1}$ such that $\text{Cert}_{\mathbb{Z}}(b(-cP, p, L))$.
 - NO and a point x such that $P(x) = 0$, or a segment $[\ell, r]$ such that $P(\ell)P(r) < 0$.
- **Procedure:**
 - Compute $c \in \mathbb{N} \setminus \{0\}$ such $b(cP, p, -1, 1) \in \mathbb{Z}^{p+1}$ using (7) (and Remark 15)
 - Initialization: $M := \{[-1, 1], c, b(cP, p, -1, 1)\}$, $N := \emptyset$, $N' = \emptyset$.
 - Isolation Phase: While L is non-empty,
 - Remove an element $[[\ell, r], c, b(cP, p, \ell, r)]$ from M .
 - If $b_0 = 0$ return NO and $[\ell]$.
 - If $b(cP, p, \ell, r)_p = 0$ return NO and $[r]$.
 - If $b(cP, p, \ell, r)_0 b(cP, p, \ell, r)_p < 0$, return NO and $[\ell, r]$.
 - If $\text{Var}(b(cP, p, \ell, r)) = 0$,
 - if $b(cP, p, \ell, r)_0 > 0$ and $b(cP, p, \ell, r)_p > 0$, add $[[\ell, r], c, b(cP, p, \ell, r)]$ to N ,
 - if $b(cP, p, \ell, r)_0 < 0$ and $b(cP, p, \ell, r)_p < 0$, add $[[\ell, r], c, b(cP, p, \ell, r)]$ to N' .
 - Else let $m = (\ell + r)/2$, compute $b(2^p cP, p, \ell, m)$ and $b(2^p cP, p, m, r)$, using Algorithm 2 with input $b(cP, p, \ell, r)$, and add
$$([\ell, m], 2^p c, b(2^p cP, p, \ell, m)), ([m, r], 2^p c, b(2^p cP, p, m, r))$$
to M .
 - Compression Phase. Initialize $T := \emptyset$. If $N' = \emptyset$, let $M := N$. If $N = \emptyset$, let $M := -N'$ obtained by replacing, in each $[[\ell, r], c, b]$ in N , c by $-c$ and b by $-b$.
 - While $M \neq \emptyset$,
 - If M has one single element $[[\ell, r], c, b(cP, p, \ell, r)]$, place it at the end of T .
 - Otherwise, remove the two first element $[[\ell, r], c, b(cP, p, \ell, r)]$ and $[[m, r], c, b(cP, p, m, r)]$ from M .

- Apply Algorithm 2 to $[[\ell, r], c, b(cP, p, \ell, r)]$ and m to get $b(c'P, p, \ell, m)$.
- If $\text{Var}(b') = 0$, place $[[\ell, m], c', b(c'P, \ell, m)]$ at the beginning of M .
- Otherwise, place $[[\ell, r], c, b(cP, p, \ell, r)]$ and $[[r, m], C, b(CP, p, r, m)]$ at the end of T .
- If $N := \emptyset$, return POS and $T = b(cP, p, L)$.
- If $N' := \emptyset$, return NEG and $T = b(-cP, p, L)$.

Example 19. Let us explain the process of Algorithm 4 for $P = X^4 + 64X^2 - 16X + 1$.

- $\text{Var}(b(3P/2, 4, -1, 1) = [123, 12, -29, -12, 752]) = 2$, it is necessary to refine $[-1, 1]$.
- $\text{Var}(b(3P, 4, -1, 0) = [246, 135, 59, 15, 3]) = 0$, $\text{Var}(b(3P, 4, 0, 1) = [3, -9, 11, 63, 150]) = 2$, it is necessary to refine $[0, 1]$.
- $\text{Var}(b(3 \cdot 2^4P, 4, 0, 1/2) = [48, -48, -16, 144, 435]) = 2$, it is necessary to refine $[0, 1/2]$, while $\text{Var}(b(3 \cdot 2^4P, 4, 1/2, 1) = [435, 726, 1148, 1704, 2400]) = 0$.
- $\text{Var}(b(3 \cdot 2^8P, 4, 0, 1/4) = [768, 0, -256, 0, 771]) = 2$, it is necessary to refine $[0, 1/4]$, while $\text{Var}(b(3 \cdot 2^8P, 4, 1/4, 1/2) = [771, 1542, 2828, 4632, 6960]) = 0$.
- The isolation phase stops since $\text{Var}(b(3 \cdot 2^{12}P, 4, 0, 1/8) = [12288, 6144, 2048, 0, 3]) = 0$, and $\text{Var}(b(3 \cdot 2^{12}P, 4, 1/8, 1/4) = [3, 6, 2060, 6168, 12336]) = 0$.

So we obtained a certificate of positivity for P

$$\begin{aligned} & [[-1, 0], \quad 3, \quad [246, 135, 59, 15, 3]], \\ & [[0, 1/8], \quad 3 \cdot 2^{12}, \quad [12288, 6144, 2048, 0, 3]], \\ & [[1/8, 1/4], \quad 3 \cdot 2^{12}, \quad [3, 6, 2060, 6168, 12336]] \\ & [[1/4, 1/2], \quad 3 \cdot 2^8, \quad [771, 1542, 2828, 4632, 6960]], \\ & [[1/2, 1], \quad 3 \cdot 2^4, \quad [435, 726, 1148, 1704, 2400]]. \end{aligned}$$

In the last step, this certificate is compressed in

$$\begin{aligned} & [[-1, 0], \quad 3, \quad [246, 135, 59, 15, 3]], \\ & [[0, 1/8], \quad 3 \cdot 2^{12}, \quad [12288, 6144, 2048, 0, 3]], \\ & [[1/8, 1], \quad 3 \cdot 2^{12}, \quad [3, 24, 100544, 302592, 614400]]. \end{aligned}$$

□

Let as before p be the degree of P , ν the bit-size of $p + 1$ and τ a bound on the bit-size of the coefficients of P . It is clear that, when running Algorithm 3 with input P , storing in N (resp. N') the values of $([\ell, r], c, b)$ such that $\text{Var}(b) = 0$ in Algorithm 3 and outputting NO and $([\ell, r], c, b)$ when $\text{Var}(b) = 1$ provides a correct output to Algorithm 4, so we can conclude using Proposition 17:

Proposition 20. *The number of applications of Algorithm 2 in the Isolation Phase of Algorithm 4 is at most $2(2\tau + 3\nu + 3)q$.*

Theorem 21. *Let $P \in \mathbb{Z}[X]$ be a square free univariate polynomial of degree p with coefficients of bit-size bounded by τ .*

The binary complexity of Algorithm 4 is $O(p^5(\tau + \log_2 p)^2)$.

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

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

If there exist $x, y \in [-1, 1]$ such that $P(x) \leq 0$ and $P(y) \geq 0$, Algorithm 4 provides rational numbers ℓ, r with numerator and denominator of bit size at most $O(p^2(\tau + \log_2 p))$ such that $P(\ell) = 0$ or $P(r) = 0$ or $P(\ell)P(r) < 0$.

Proof:

For the case where $P > 0$ on $[-1, 1]$, there are $O(p(\tau + \log_2 p))$ calls to Algorithm 2 in the Isolation Phase. The bit-size of the Bernstein coefficients in each node is $O(p^2(\tau + \log_2 p))$ by Corollary 16, 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 $O(p(\tau + \log_2 p))$ by Proposition 17. Moreover there are $O(p^2)$ additions to perform at each node. In the compression phase, there are $O(p(\tau + \log_2 p))$ calls to Algorithm 2, the number of arithmetic operations is $O(p^2)$ in each call and the bit-size of the integers are $O(p^2(\tau + \log_2 p))$.

It is clear that the total number of coefficients in $b(cP, p, L)$ is $O(p^2)$, given that each node contains $p + 1$ coefficients and there are at most $p + 1$ intervals output by Remark 8. Finally, given the estimates on the bit-sizes of the coefficients, 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 where there exists $x, y \in [-1, 1]$ such that $P(x) \leq 0$ and $P(y) \geq 0$ is clear given the bit-size estimates of the coefficients. \square

4. THE GENERAL CASE

In the general case, let us explain roughly the method we use: we compute first a square free decomposition of P , then a certificate of positivity for each element of this square free decomposition of P , and finally obtain a decomposition of $[-1, 1]$ in subintervals on which the expression of P in the Bernstein basis of this interval provides a certificate of positivity in the case where $P > 0$ on $[-1, 1]$.

A square free decomposition of a polynomial $P \in \mathbb{Z}[X]$ is given by square free, non constant, pairwise coprime, polynomials P_1, \dots, P_k of $\mathbb{Z}[X]$, of respective degree p_i such that $P = P_1 P_2^2 \dots P_k^k$. There are several algorithms providing a square free decomposition, Yun's Algorithm below is considered as quite efficient one.

Algorithm 5. [Yun's square free decomposition algorithm]

- **Input:** a non-zero monic polynomial $P \in \mathbb{Z}[X]$.
- **Output:** square free, non constant, pairwise coprime, polynomials P_1, \dots, P_k in $\mathbb{Z}[X]$ of respective degree p_i such that $P = P_1 P_2^2 \dots P_k^k$.
- **Procedure:**
 - Initialization: $G := \gcd(P, P')$, $C_1 := P/G$, $D_1 := P'/G - C_1$, $i := 1$, $F := \emptyset$.
 - While $\deg(C_i) \neq 0$, add $Q_i := \gcd(C_i, D_i)$ to F , $C_{i+1} := C_i/Q_i$, $D_{i+1} := D_i/Q_i - C'_{i+1}$, $i := i + 1$.

Proof of correctness:

We prove by induction on i that

- $C_i = P_1 \dots P_k$,
- $D_i = \sum_{j=1}^{k-i} j P_{i+1} \dots P_{i+j-1} P'_{i+j} P_{j+i+1} \dots P_k$,
- $P_i = Q_i$.

For $i = 1$, $G = \gcd(P, P') = P_2 P_3^2 \dots P_k^{k-1}$: indeed $P_2 P_3^2 \dots P_k^{k-1}$ divides P and P' , and it is clear that P_1^i does not divide $P' = \sum_{i=1}^k j P_1 \dots P_{j-1} P'_j P_{j+1} \dots P_k$. Thus $C_1 = P/G = P_1 \dots P_k$, and

$$\begin{aligned} D_1 = P'/G - C'_1 &= \sum_{j=1}^k j P_1 \dots P_{j-1} P'_j P_{j+1} \dots P_k - \sum_{j=1}^k P_1 \dots P_{j-1} P'_j P_{j+1} \dots P_k \\ &= \sum_{j=1}^k j P_2 \dots P_j P'_{j+1} P_{j+2} \dots P_k. \end{aligned}$$

Finally $Q_1 = \gcd(C_1, D_1) = P_1$ since P_1 divides C_1 and D_1 , P_1^2 does not divide C_1 , and P_j does not divide D_1 , $j > 1$.

We suppose that the claim is true for i and prove it for $i + 1$. We have $C_{i+1} = C_i/Q_i = P_{i+1} \dots P_k$, and

$$\begin{aligned} D_{i+1} = D_i/Q_i - C_i' &= \sum_{j=1}^{k-i} j P_{i+1} \dots P_{i+j-1} P_{i+j}' P_{i+j+1} \dots P_k - \sum_{j=i}^{k-i} P_i \dots P_{i+j-1} P_{i+j}' P_{i+j+1} \dots P_k \\ &= \sum_{j=1}^{k-i-1} j P_{i+2} \dots P_{i+j} P_{i+1+j}' P_{j+i+2} \dots P_k. \end{aligned}$$

Finally $Q_{i+1} = \gcd(C_{i+1}, D_{i+1}) = P_{i+1}$ since P_i divides C_i and D_i , P_i^2 does not divide C_i , and P_j does not divide D_i , $j > i$. \square

Complexity analysis:

Let as before p be the degree of P , ν the bit-size of $p + 1$ and τ a bound on the bit-size of the coefficients of P .

The degrees of all the polynomials computed are bounded by p . The number of arithmetic operations for each gcd is $O(p^2)$, as well as for each Euclidean division, so the total number of arithmetic operations is clearly estimated by $O(k p^2) \leq O(p^3)$.

By Corollary 10, the bit-size of P_i and C_i is at most $\tau + p_i + \nu$, and it is not difficult to check that the bit-size of D_i is at most $2\tau + 2p + 6\nu$. Computing the gcd through subresultants [1] the intermediate computations are arithmetic operations (additions, multiplications, exact divisions) of bit-size $O(p(\tau + p))$.

Finally there are $O(k p^2)$ arithmetic operations between integer of bit-size $O(p(\tau + p))$. \square

We are now ready for the general algorithm for certificates of positivity.

Algorithm 6. [Certificate of positivity]

- **Input:** a non-zero polynomial $P \in \mathbb{Z}[X]$
- **Output:**
 - POS if $P > 0$ on $[-1, 1]$, with a rational subdivision L of $[-1, 1]$ of length $n \leq p$, and $c \in (\mathbb{N}^*)^{n+1}$ such that $\text{Cert}_{\mathbb{Z}}(b(cP, p, L))$.
 - NEG if $P < 0$ on $[-1, 1]$, with a rational subdivision L of $[-1, 1]$ of length $n \leq p$, and $c \in (\mathbb{N}^*)^{n+1}$ such that $\text{Cert}_{\mathbb{Z}}(b(-cP, p, L))$.
 - NO if there are values $x \in [-1, 1]$ such that $P(x) \leq 0$, together with a value x such that $P(x) \leq 0$, or a segment $[\ell, r]$ and a divisor Q of P such that $Q(\ell) Q(r) < 0$.
- **Procedure:**
 - Compute the square free decomposition P_1, \dots, P_k of P .
 - For every i from 1 to k apply Algorithm 4 with input P_i .
 - If there exists $i \leq k$ such that the output of Algorithm 4 contains NO, output the divisor P_i and
 - the value x equal to ℓ_i or r_i such that $Q(x) = P(x) = 0$,
 - the segment $[\ell_i, r_i]$ such that $P_i(\ell_i) P_i(r_i) < 0$,
obtained at the end of Algorithm 4 applied to P_i .
 - Otherwise
 - let $L = [\ell_0, \dots, \ell_n]$, $\ell_0 = -1 < \dots < \ell_n = 1$ be the smallest subdivision refining the subdivisions L_i output by Algorithm 4 applied to P_i .
 - let $\varepsilon = (-1)^j$, where j is the number of natural numbers $\leq k$ such that the output of Algorithm 4 with input P_i contains NEG.
 - compute $c_0 \in \mathbb{N} \setminus \{0\}$ such that the elements of $b_0 = b(c_0 P, -1, 1) \in \mathbb{Z}^{p+1}$ using (1), and Remark

- for every $i = 1, \dots, n$ compute c_i such that $b_i = b(c_i P, p, \ell_{i-1}, \ell_i) \in \mathbb{Z}^{p+1}$, applying Algorithm 2 to $b(c_{i-1} P, \ell_{i-1}, 1)$, and ℓ_i .
- add the result $([\ell_{i-1}, \ell_i], c_i, b_i)$ to
 - Pos(P) if $\varepsilon = 1$,
 - Neg(P) if $\varepsilon = -1$.

Correctness:

The fact that $\text{Cert}(P, b(P, p, L))$ follows from Remark 1.

For the case where there exists a leaf of T such that there exists i such that $P_i(\ell) P_i(r) \leq 0$, there are three cases:

- if $P_i(\ell) = 0$, then $P(\ell) = 0$,
- if $P_i(r) = 0$, then $P(r) = 0$,
- if $P_i(\ell) P_i(r) < 0$, then there exist $x \in (\ell, r)$ such that $P_i(x) = 0$, hence $P(x) = 0$. □

Theorem 22. *Let $P \in \mathbb{Z}[X]$ be a univariate polynomial of degree p with coefficients of bit-size bounded by τ .*

If $P > 0$ on $[-1, 1]$, Algorithm 6 gives a certificate of positivity of bit-size $O(p^4(\tau + \log_2 p))$.

If $P < 0$ on $[-1, 1]$, Algorithm 6 gives a certificate of negativity of bit-size $O(p^4(\tau + \log_2 p))$.

If there exist $x, y \in [-1, 1]$ such that $P(x) \leq 0$ and $P(y) \geq 0$, Algorithm 6 provides an interval $[\ell, r]$ with rational endpoints with numerator and denominator of bit size at most $O(p(\tau + \log_2 p))$ and a divisor Q of P such that $Q(\ell) Q(r) \leq 0$.

Proof:

For the case where $P > 0$ on $[-1, 1]$, there are $O(p)$ intervals which are considered. It is thus clear that the total number of coefficients in $b(c P, p, L)$ is $O(p^2)$. The bit-size of the Bernstein coefficients in each node is $O(p^2(\tau + \log_2 p))$ by Corollary 16, 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 $O(p(\tau + \log_2 p))$ by Proposition 17. Finally the bit-size of the certificate of positivity is at most $O(p^4(\tau + \log_2 p))$ when $P > 0$ on $[-1, 1]$.

When there exists $x \in [-1, 1]$ such that $P(x) \leq 0$, this is detected by Algorithm 4 at a point y which is a rational number with numerators and denominators of bit size at most $O(p(\tau + \log_2 p))$. The statement in the case where there exists $x, y \in [-1, 1]$ such that $P(x) \leq 0$ and $P(y) \geq 0$ is clear. □

5. COMPARISON BETWEEN THE SIZE OF THE TWO KINDS OF CERTIFICATES OF POSITIVITY

A quantitative bound on the Bernstein degree was proved in [7], namely

$$\frac{p(p-1)}{2} \frac{M}{\lambda} \tag{8}$$

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 Bernstein coefficients of P on $[-1, 1]$.

5.1. Estimates on the minimum of a polynomial.

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

Theorem 23. *The minimum of P is at least $2^{-2p(1+\tau+\nu)+(\tau+1)}$.*

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

$$Q(Y) = \prod_{z \in Z_{\varepsilon\tau}(P', \mathbb{C})} Y - P(z),$$

whose roots are the values of P at the roots of P' .

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

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

where

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

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

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

The proof of Theorem 23 relies on two lemmas

Lemma 24. *Let M be a square matrix of size $2p - 1$ whose $(p - 1)$ first rows contain at most $p + 1$ non zero coefficients with absolute value estimated by 2^τ , and whose p last rows contain at most p non zero coefficients with absolute value estimated by $p2^\tau$. Then*

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

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

$$|\det(M)| \leq \sqrt{((p+1)2^{2\tau})^{p-1} (p p^2 2^{2\tau})^p}.$$

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

Lemma 25. *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

$$f: \{1, \dots, p-1\} \rightarrow \{0, 1\}$$

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

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

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

The coefficient of Y^i in Q is the sum of at most 2^{p-1} determinants S_f . Applying Lemma 24, we get that the coefficients of Q are bounded by

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

Proof of Theorem 23: According to Cauchy' bound [1], the root with smallest absolute value λ of

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

is bigger than $\left(\sum_{q \leq i \leq p-1} \left| \frac{c_i}{c_q} \right| \right)^{-1}$. Using Lemma 25,

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

Remark 26. Our result is very slightly better than a recent result due to Bugeaud and Mignotte [4]. □

Example 27. Following a suggestion by Bugeaud and Mignotte [4], we consider the family of polynomials

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

For every k, p , the minimum of $A(k, p)$ is close to the estimation of Theorem 23 [4]. Indeed, $\tau = k - 1$, and the minimum of $A(k, p)$ is smaller than the value $2^{-2p(\tau-1)}$ obtained at $x = 2^{-k}$, and depends exponentially on p and τ . □

5.2. Comparison between the size of certificates of positivity.

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

$$p(p-1) 2^{p(2\tau+3\nu+3)+\nu+2}, \quad (9)$$

using the estimation on λ given by Theorem 23 and $L \leq 2^{p\nu+p+\tau+\nu}$, by Corollary 14. Note that the bound given by (9) is exponential in τ and p while the bound of Theorem 22 is polynomial in τ and p .

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

5.2.1. Size of certificates of positivity with respect to the bit-size.

Powers and Reznick's bound (8) is sharp, as proved [7] where they provide a family of polynomials of degree 2 index by $k \in \mathbb{N}$, namely

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

for which the Bernstein degree is precisely $2^k - 1$. More precisely, they describe a family for which the Polya degree is $2^k - 3$, giving the family P_k by the Goursat transform. 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 certificate of positivity given by Theorem 22 is particularly short since it is linear in $\tau = k$. More precisely our certificate of positivity for P_k is the following

$$[[-1, 0], 1, [2^k, 1, 1]], [[0, 1], 1, [1, 1, 2^k]]$$

which means

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

5.2.2. 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

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

introduced earlier has a minimum very close to the bound of Theorem 23 and appears thus as a good test family for the comparison between the size of the certificate of positivity given by Theorem 22 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,
- when $p = 2$, the Bernstein degree is 82, the coefficients of $1311795 A(1, 2)$ in the Bernstein basis of degree 82 for $-1, 1$ are

[13117950, 12606030, 12109910, 11629116, 11163186, 10711670, 10274130, 9850140, 9439286, 9041166, 8655390, 8281580, 7919370, 7568406, 7228346, 6898860, 6579630, 6270350, 5970726, 5680476, 5399330, 5127030, 4863330, 4607996, 4360806, 4121550, 3890030, 3666060, 3449466, 3240086, 3037770, 2842380, 2653790, 2471886, 2296566, 2127740, 1965330, 1809270, 1659506, 1515996, 1378710, 1247630, 1122750, 1004076, 891626, 785430, 685530, 591980, 504846, 424206, 350150, 282780, 222210, 168566, 121986, 82620, 50630, 26190, 9486, 716, 90, 7830, 24170, 49356, 83646, 127310, 180630, 243900, 317426, 401526, 496530, 602780, 720630, 850446, 992606, 1147500, 1315530, 1497110, 1692666, 1902636, 2127470, 2367630, 2623590]

while our certificate of positivity is

[[[-1, 0], 3, [30, 18, 11, 6, 3]], [[0, 1/2], 48, [48, 24, 8, 0, 3]], [[1/2, 1], 48, [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 $X^{2p} = X^{2p}(X + (1 - X))^{2N-2p}$,

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

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

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

Let us prove that

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

or equivalently

$$(N-1)\dots(N-2p+1) < 2(2N-2)\dots(2N-2p+1) \quad (10)$$

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

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

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

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

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

So, if $2N-2p < 2^{2p}$, or equivalently $N < 2^{2p-1} + p$, (10) 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 Algorithm 2 and so the Bernstein degree of $A(1, p)$ is bigger than $2^{2p} + 2p - 1$.

5.3. Global positivity certificates.

We now explain how the various local positivity certificates $b(cP, p, \ell_{i-1}, \ell_i)$ can be glued together to provide a positivstellensatz identity [9, 2] certifying that P is positive on $[-1, 1]$. The degree of this positivstellensatz identity is bounded by $2(p+1)p$ when $P \in R[X]$ where R is a general real closed field, and the bit-size is $O(p^4(\tau + \log_2 p))$ when $P \in \mathbb{Z}[X]$.

It follows from Theorem 6 that if P is positive on $[-1, 1]$, there exists a subdivision $L = [\ell_1, \dots, \ell_n]$ of $[-1, 1]$ of length $n \leq p$ such that $\text{Cert}(b(P, p, L))$. We can suppose without loss of generality that p is even (replacing p by $p+1$ if necessary) and that all the components of $b(P, p, \ell_{i-1}, \ell_i)$ are positive by Remark 1 a), doubling if necessary the number of intervals, so that $n \leq 2p+1$.

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

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

can be rewritten as

$$a_i - P + \sum_{j=0}^{p/2} (b_{2j} - a_j) \text{Bern}_{p,2j}(\ell_{i-1}, \ell_i) = - \sum_{j=1}^{p/2} (b_{2j-1} - a_j) \text{Bern}_{p,2j-1}(\ell_{i-1}, \ell_i). \quad (11)$$

Multiplying together these n identities, we obtain

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

where a is a positive number, S is a sum of squares of degree at most $(n-1)p$, T is a sum of squares of degree at most np and U is a sum of components of degree at most np of the form $Q^2(X+1)^j(1-X)^k$ with $j \leq p$, $k \leq p$.

In other words

$$a - SP + T + U = 0. \quad (12)$$

This is a positivstellensatz equality [9, 2] certifying that $P(x) > 0$ on $[-1, 1]$. Indeed, if we suppose that there existed x such that $P(x) \leq 0$, evaluating (12) at x gives a contradiction

$$c = 0$$

with c a positive constant.

Theorem 28. *If $P \in R[X]$ is > 0 on $[-1, 1]$, there exists a positivstellensatz identity*

$$a - SP + T + U = 0. \quad (13)$$

where a is a positive number, S is a sum of squares of degree at most $(2p+1)p$, T is a sum of squares of degree at most $2(p+1)p$ and U is the sum of finite number of components of degree at most $2(p+1)p$ of the form $Q^2(1-X)^j(X+1)^k$ with $j \leq p$, $k \leq p$. Moreover if $P \in \mathbb{Z}[X]$, the total bit-size in (13) is at most $O(p^4(\tau + \log_2 p))$.

Proof The only thing that remains to prove is the statement on the bit-size when $P \in \mathbb{Z}[X]$. This is an immediate consequence of the proof of Theorem 22 and of the construction of (13). \square

Remark 29. 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 [9, 2]) since by Remark 7 it is really necessary to use subdivisions with endpoints in R in the construction. \square

1. S. BASU, R. POLLACK, M.-F. ROY, *Algorithms in real algebraic geometry*, Springer-Verlag, second edition (2006). Revised version of the first edition on line at <http://perso.univ-rennes1.fr/marie-francoise.roy/>
2. J. BOCHNAK, M. COSTE, M.-F. ROY, *Real algebraic geometry*, Springer-Verlag, second edition in english (1998)
3. S. BERNSTEIN, *Sur la représentation des polynômes positifs*, Soobshch. Kharkov matem. ob-va, ser. 2, 14 (1915), 227-228.(1915)
4. Y. BUGEAUD, M. MIGNOTTE, *Private communication*, (2005)
5. F. CARUSO, *The SARAG Library*, Proceedings of the ICMS '06, Springer (2006). Stable version included in maxima: <http://maxima.sourceforge.net/>, last vesion on line at <http://perso.univ-rennes1.fr/marie-francoise.roy/bpr-posted1.html>
6. A. EIGENWILLIG, V. SHARMA, C. K. YAP, *Almost Tight Recursion Tree Bounds for the Descartes Method*, Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, Italy, ACM, New York, 2006, 71-78.(2005)
7. V. POWERS, B. REZNICK, *A new bound for Polyá's Theorem with applications to polynomials positive on polyhedra*, Journal of Pure and Applied Algebra 164, 221-229 (2001)
8. V. POWERS, B. REZNICK, *Private communication*, (2006)
9. G. STENGLE, *A Nullstellensatz and a Positivstellensatz in semialgebraic geometry*, Mathematische Annalen, 207, 87-97 (1974)