

VINCENT'S THEOREM OF 1836: OVERVIEW AND FUTURE RESEARCH

A. G. Akritas*

UDC 519.61

In this paper, we present two different versions of Vincent's theorem of 1836 and discuss various real root isolation methods derived from them: one using continued fractions and two using bisections, the former being the fastest real root isolation method. Regarding the continued fractions method, we first show how, using a recently developed quadratic complexity bound on the values of the positive roots of polynomials, its performance has been improved by an average of 40% over its initial implementation, and then we indicate directions for future research. Bibliography: 45 titles.

1. INTRODUCTION

The isolation of the real roots of a polynomial is the process of finding real disjoint intervals such that each interval contains one real root and every real root is contained in some interval.

Since the beginning of the 19th century, and according to the French “school” of mathematics, the isolation has been considered the first step in finding the real roots of a polynomial equation, the second step being the approximation of the roots to any degree of accuracy.

Sturm was the first mathematician to present a theorem, in 1829, for isolating the real roots of a polynomial using bisection, see [6]. His theorem was widely used until 1980, when it was replaced in the major computer algebra systems by versions of Vincent's theorem.

Vincent's theorem of 1836 published in [44] has a very interesting and exciting history (see [11, 12, 20–22] and [31]). This theorem was almost totally forgotten, until it was rediscovered, in 1976, by the author and formed the basis of his Ph.D. thesis [1]. Subsequently, scientists from all over the world made their own contributions to various aspects of it, so that today we can claim that we have a very good understanding of this theorem.

A short biography of Vincent (in French) can be found in p. 1026, vol. 31 of *La Grande Encyclopédie*, see <http://gallica.bnf.fr/ark:/12148/bpt6k24666x>, whereas a copy of his portrait can be seen in http://www.allposters.fr/-st/Lasnier-Affiches_c25893_s88165_.htm, [25].

Vincent's theorem depends on Descartes' rule of signs, which gives us an *upper bound* on the number of positive roots of a polynomial, see [24]. Specifically, consider a polynomial $p(x) \in \mathbb{R}[x]$, $p(x) = a_n x^n + \dots + a_1 x + a_0$, and let $\text{var}(p)$ represent the number of sign *variations* or *changes* (positive to negative and vice versa) in the sequence of coefficients a_n, a_{n-1}, \dots, a_0 .

Descartes' rule of signs. The number $\varrho_+(p)$ of real roots (multiplicities counted) of a polynomial $p(x) \in \mathbb{R}[x]$ in the open interval $]0, +\infty[$ is bounded above by $\text{var}(p)$; that is, we have $\text{var}(p) \geq \varrho_+(p)$.

According to Descartes' rule of signs, $\text{var}(p) = 0$ implies $\varrho_+(p) = 0$.

Additionally, according to Descartes' rule of signs, the mean value theorem, and the fact that polynomial functions are continuous, $\text{var}(p) = 1$ implies $\varrho_+(p) = 1$, see [24].

Therefore, Descartes' rule of signs yields the *exact* number of positive roots *only* in the two special cases mentioned above.¹

These two special cases of Descartes' rule are used in both versions of Vincent's theorem of 1836, which are described below.

The rest of the paper is structured as follows.

In Sec. 2, we present the two versions of Vincent's theorem and provide a sketch of one of its proofs.

In Sec. 3, we explain how Vincent's theorem can be used to isolate the real roots of polynomials and describe the continued fractions method and two bisections methods derived from it.

In Sec. 4, we present recently developed, by us, linear and quadratic complexity bounds on the values of the positive roots of polynomials and elaborate on their impact on the performance of the continued fractions method.

Finally, there is a conclusion, where we indicate directions for future research.

*Department of Computer and Communication, Engineering University of Thessaly, Greece, e-mail: akritas@uth.gr.

¹These two special cases were known to Cardano; in other words, what Descartes did was to generalize “Cardano's *special* rule of signs.” This detail is mentioned in [6].

2. THE TWO DIFFERENT VERSIONS OF VINCENT'S THEOREM

We begin with Vincent's original version, which was published in the first issue (1836) of the French *Journal of Pure and Applied Mathematics*.

Theorem 1 (Vincent's theorem, "continued fractions" version, 1836). *Given a polynomial $p(x)$ of degree n with rational coefficients and without multiple roots, if we sequentially perform replacements of the form*

$$x \leftarrow \alpha_1 + \frac{1}{x}, \quad x \leftarrow \alpha_2 + \frac{1}{x}, \quad x \leftarrow \alpha_3 + \frac{1}{x}, \dots,$$

where $\alpha_1 \geq 0$ is an arbitrary nonnegative integer and $\alpha_2, \alpha_3, \dots$ are arbitrary positive integers, $\alpha_i > 0$, $i > 1$, then the resulting polynomial has either no sign variations or one sign variation. In the latter case, the equation has exactly one positive root, which is represented by the continued fraction

$$\alpha_1 + \frac{1}{\alpha_2 + \frac{1}{\alpha_3 + \frac{1}{\ddots}}},$$

whereas in the former case, there are no positive roots.

The negative roots are treated in the same way as suggested by Sturm – after we transform them into positive ones by the replacement $x \leftarrow -x$ performed on $p(x)$. The requirement that $p(x)$ have no multiple roots does not restrict the generality of the theorem, because in the opposite case we first apply the square-free factorization and then isolate the roots of each of the square-free factors.

This theorem was kept "alive" by Uspensky in his book [42] of 1948, where it was rediscovered by the author and formed the subject of his Ph.D. thesis [1]. For a detailed discussion of the theorem, its extension, the geometrical interpretation of the transformations involved, and three different proofs, see [20–22]; a fourth proof is presented by Ostrowski [33], who rediscovered a special case of a previously stated theorem by Obreschkoff [32, p. 81]. We sketch an outline of one of the proofs after presenting the second version of the theorem.

In 2000, Alesina and Galuzzi published the so-called *bisection version* of Vincent's theorem, [20–22]. This modern version is stated as follows.

Theorem 2 (Vincent's theorem, "bisection" version, 2000). *Let $p(x)$ be a real polynomial of degree n that has only simple roots. One can determine a positive quantity δ so that for every pair of positive real numbers a and b with $|b - a| < \delta$, every transformed polynomial of the form*

$$f(x) = (1 + x)^n p\left(\frac{a + bx}{1 + x}\right)$$

has exactly 0 or 1 variations. The second case is possible if and only if $p(x)$ has a simple root within $]a, b[$.

Sketch of a proof. The proof by Alesina and Galuzzi is the most recent and, in the author's opinion, the most elegant of all existing proofs of Vincent's theorem.

To prove the theorem, Alesina and Galuzzi show that after a series of transformations (bisections) mentioned in Theorem 1 (Theorem 2), a polynomial with one positive root will eventually have one sign variation, see Fig. 1. To show this, they use the following theorem by Obreschkoff, of 1920–1923, which gives necessary conditions under which a polynomial with one positive root has exactly one sign variation in the sequence of its coefficients, see [32].²

Theorem 3 (Obreschkoff's cone or sector theorem, 1920–1923). *If a real polynomial has one simple root x_0 , and all the other (possibly multiple) roots lie in the sector*

$$S_{\sqrt{3}} = \{x = -\alpha + i\beta \mid \alpha > 0 \text{ and } \beta^2 \leq 3\alpha^2\},$$

then the sequence of its coefficients has exactly one sign variation.

²This is actually Obreschkoff's theorem for the special case where the number of sign variations equals one.

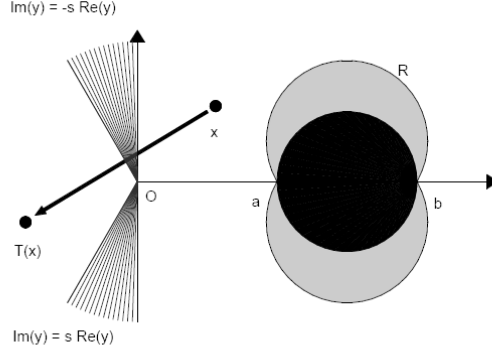


FIG. 1. Obreschkoff's cone or sector theorem of 1920–1923, [22].

3. POLYNOMIAL REAL ROOT ISOLATION WITH VINCENT'S THEOREM

By cleverly utilizing the two special cases of Descartes' rule, the cases of 0 or 1 sign variations, both versions of Vincent's theorem can be used to isolate the positive roots of a given polynomial $p(x)$. To see this, note that if we consider the Möbius transformation $M(x) = \frac{ax+b}{cx+d}$ corresponding to the continued fraction that leads to a transformed polynomial

$$f(x) = (cx + d)^n p\left(\frac{ax + b}{cx + d}\right) \quad (1)$$

with one sign variation, then the single positive root of $f(x)$ – in the interval $]0, +\infty[$ – corresponds to *that* positive root of $p(x)$ that lies in the open interval with endpoints $\frac{b}{d}$ and $\frac{a}{c}$. These endpoints are *not* ordered and correspond to $M(0)$ and $M(\infty)$, respectively.³

Therefore, to isolate the positive roots of a polynomial, all we have to do is compute for *each* root the variables a, b, c, d of the corresponding Möbius transformation $M(x) = \frac{ax+b}{cx+d}$ that leads to a transformed polynomial $f(x) = (cx + d)^n p\left(\frac{ax+b}{cx+d}\right)$ with one sign variation.

Crucial observation 1. As we will see in the sequel, the variables a, b, c, d of the Möbius transformation $M(x) = \frac{ax+b}{cx+d}$ (in Vincent's theorem) leading to a transformed polynomial with one sign variation can be computed

- *either via continued fractions*, which leads to the continued fractions method developed by Akritas and Strzeboński, which is called the Vincent–Akritas–Strzeboński (VAS) *continued fractions* method.⁴
- *or via bisection*, which leads to two *bisection* methods: the first one was developed by Collins and Akritas and is called the Vincent–Collins–Akritas (VCA) *bisection* method,⁵ whereas the second one was developed by Alesina and Galuzzi and is called the Vincent–Alesina–Galuzzi *bisection* method.⁶

It should be noted that the VCA bisection method was first developed in 1976 by Collins and Akritas [27], and that its fastest implementation was developed in 2004 by Rouillier and Zimmermann [34]. The VAS continued fractions method was developed later, in 1978 by Akritas [2, 3], and in 1994 by Akritas, Botcharov, and Strzeboński [10]. Its fastest implementation was developed in 2008 by Akritas, Strzeboński, and Vigklas [19].

At this point, the inquisitive reader might ask why not use numeric methods instead of the symbolic ones mentioned above. The answer is twofold:

- numeric methods *cannot* isolate just the positive roots; they isolate *all* roots, both real and complex; and
- numeric methods can give wrong answers, as the following example demonstrates.

³As can be seen elsewhere ([7]), the endpoints can also be computed from $M(0)$ and $M(1)$ if we work in the interval $]0, 1[$; in that case, Descartes' rule of signs does not apply and we use Uspensky's test instead.

⁴To distinguish it from other continued fraction methods, such as [13, 26, 40] cited in [45, pp. 470–478]. In [37], VAS is referred to as the “Akritas' continued fractions method.” See also [20] and [23].

⁵Erroneously referred to in the literature either as “modified Uspensky's method” (1976–1986), [5], or as “Descartes' method” (1986–2006), [7].

⁶To distinguish them from Sturm's bisection method [45].

Example 1. Consider the polynomial

$$10^{999}(x-1)^{50}-1$$

whose real roots we want to isolate (it has only two, both positive and $\neq 1$). We solve this example using different versions of *Mathematica*:

- *Mathematica* 5 or 6. In this case,
 - a numeric method using 1010 digits takes *56ms* and fails to find all 50 roots equal to 1;
 - a numeric method using 1020 digits successfully isolates *all fifty* roots, but takes *18000ms*;
 - the VAS continued fractions method discussed below takes *4ms* to isolate the two real roots.
- *Mathematica* 7. In this case,
 - as can be seen in Fig. 2, the improved numeric method used in Mma 7 takes *12.933 seconds* to find the two positive roots with 30 digits of accuracy;
 - on the other hand, as can be seen in Fig. 3, the function `RootIntervals`, i.e., the VAS *continued fractions method*, isolates the two positive roots in *0.015 seconds*;
 - ... and the function `FindRoot` approximates them to 30 digits of accuracy in practically no time at all!

Having made clear the need for the above-mentioned symbolic real root isolation methods, we proceed to their description.

[illegible]

FIG. 2. Using the function `NRoots` in Mma 7 to numerically compute the two roots.

```
ints = RootIntervals[f][[1]] // Timing  
  
{0.015, {{0, 1}, {1, 2}}}  
  
ints = Last[ints]  
  
{{0, 1}, {1, 2}}  
  
FindRoot[f, {x, #[[1]], #[[2]]}, Method → Brent,  
WorkingPrecision → 30, MaxIterations → 200] &/@ints // Timing  
  
{5.42101 × 10-19,  
{{x → 0.9999999999999999999999989528714519}, {x → 1.0000000000000000000000001047128548}}}
```

FIG. 3. Using the function `RootIntervals`, the VAS continued fractions method, to isolate the roots and the function `FindRoot` to approximate them, in Mma 7.

3.1. The continued fractions method derived from Vincent's theorem

The VAS continued fractions method is a *direct* implementation of Vincent’s theorem. It was originally presented by Vincent [44] in 1836 in an “exponential” form; namely, Vincent computed each partial quotient a_i by a series of *unit* increments $a_i \leftarrow a_i + 1$, which are equivalent to substitutions of the form $x \leftarrow x + 1$.

In 1978, the method was converted into its “polynomial” form by Akritas, who in his Ph.D thesis [1] computed each partial quotient a_i as a lower bound, ℓb , on the values of the positive roots of a polynomial – the so-called “ideal” positive lower root bound, which computes the integer part of the smallest positive root, see [16]; that

is, we now set $a_i \leftarrow \ell b$, or, equivalently, we perform the substitution $x \leftarrow x + \ell b$, which takes about the same time as the substitution $x \leftarrow x + 1$. For details, also see [2–4] and [6, Chap. 7].

Finally, since the ideal positive lower root bound does not exist, Strzeboński [14] introduced the substitution $x \leftarrow \ell b_{\text{computed}} \cdot x$, whenever $\ell b_{\text{computed}} > 16$, where, in general, $\ell b > \ell b_{\text{computed}}$ and the value 16 was determined experimentally.

In [14], it was also shown that the VAS continued fractions method is faster than the fastest implementation of the VCA bisection method [34], a result which was independently confirmed by Tsigaridas and Emiris [41]; also see [17]. In 2007, Sharma [36, 37] removed the hypothesis of the ideal positive lower bound and proved that VAS is still polynomial in time!

In Algorithm 1, we present a recursive description of the VAS continued fractions method. We follow [24], which pedagogically seems to be the most appropriate style of presentation:

THE VAS CONTINUED FRACTIONS METHOD

Input: A univariate, square-free polynomial $p(x) \in \mathbb{Z}[x]$, $p(0) \neq 0$, and the Möbius transformation $M(x) = \frac{ax+b}{cx+d} = x$, $a, b, c, d \in \mathbb{Z}$.
Output: A list of isolating intervals for the *positive* roots of $p(x)$.

```

1  var  $\leftarrow$  the number of sign changes of  $p(x)$ ;
2  if var = 0 then RETURN  $\emptyset$ ;
3  if var = 1 then RETURN  $\{[a, b] // a = \min(M(0), M(\infty)),$ 
    $b = \max(M(0), M(\infty))\}$ ;
4   $b \leftarrow$  a lower bound on the positive roots of  $p(x)$ ;
5  if  $\ell b > 1$  {  $p \leftarrow p(x + \ell b)$ ,  $M \leftarrow M(x + \ell b)$  };
6   $p_{01} \leftarrow (x+1)^{\deg(p)} p(\frac{1}{x+1})$ ,  $M_{01} \leftarrow M(\frac{1}{x+1}) //$ 
   Look for real roots in  $]0, 1[$ ;
7   $m \leftarrow M(1) //$  Is 1 a root?;
8   $p_{1\infty} \leftarrow p(x+1)$ ,  $M_{1\infty} \leftarrow M(x+1) //$  Look for real roots in  $]1, +\infty[$ ;
9  if  $p(1) \neq 0$  then
10 | RETURN  $\text{VAS}(p_{01}, M_{01}) \cup \text{VAS}(p_{1\infty}, M_{1\infty})$ 
11 else
12 | RETURN  $\text{VAS}(p_{01}, M_{01}) \cup \{[m, m]\} \cup \text{VAS}(p_{1\infty}, M_{1\infty})$ 
13 end
```

Algorithm 1. The VAS (p, M) “*continued fractions*” algorithm, where the second argument is the Möbius transformation $M(x)$ associated with $p(x)$. For simplicity, Strzeboński’s contribution is not included.

The VAS continued fractions method has been implemented in the computer algebra system *Mathematica*, and, as we will see in the sequel, for the Mignotte polynomials it is several *thousand* times *faster* than the fastest implementation of the VCA bisection method (also see Fig. 4).

Please note that the VAS continued fractions method uses Descartes’ rule of signs as a termination test (lines 1–3) and that it relies heavily on the *repeated* estimation of lower bounds on the values of the positive roots of polynomials (line 4). It should be emphasized that the efficiency of VAS depends on how good these estimates are – a fact that is exploited in the sequel (Sec. 4). Moreover, note the following:

- If we remove lines 4 and 5 from $\text{VAS}(p, M)$, we are left with an exponential algorithm.
- Any substitution performed on the polynomial $p(x)$ is also performed on its associated Möbius transformation $M(x)$ (lines 5, 6, and 8).
- To isolate the real roots of $p(x)$ in the open interval $]0, +\infty[$, we proceed as follows:
 - we first isolate the real roots in the interval $]0, 1[$ (lines 6 and 10 (or 12)),
 - we then deal with the case where 1 is a root of $p(x)$ (lines 7, 9, and 12),
 - and, finally, we isolate the real roots in the interval $]1, +\infty[$ (lines 8 and 10 (or 12)).
- The isolating intervals are computed from the Möbius transformations in line 3 except for the integer roots which are computed in lines 7 and 12.

[illegible]

Using the plausible hypothesis of the “*ideal*” lower bound on the values of the positive roots along with the fast translation algorithm by von zur Gathen and Gerhard [29], the computing time of the VAS continued fractions method is

However, the use of the plausible hypothesis mentioned above did *not* go unchallenged, and it was a widely held belief that if it were removed, then the computing time of the VAS continued fractions method would be exponential! This resulted in people shying away from VAS ignoring that:

And all that using Cauchy's bound (the only one available then, but also one of the worst, as we will see in Sec. 4) to compute the lower bounds on the values of the positive roots!

$$O(n^8 \tau^3),$$

3.2. The two bisection methods derived from Vincent's theorem

The *first* bisection method derived from Vincent's theorem, VCA, was developed in 1976, by Collins and Akritas [27], in an attempt to improve the exponential behavior of Vincent's original continued fractions algorithm. It uses Uspensky's termination criterion (explained below) and bisects the interval $]0, 1[$.

Let $p(x)$ be a polynomial whose roots we want to isolate, and let ub be an upper bound on the values of its positive roots. Then all the positive roots of $p(ub \cdot x)$ lie in the interval $]0, 1[$, and the VCA method isolates them by repeatedly bisecting the interval $]0, 1[$, while using an appropriate “*criterion*” to make inferences about the number of positive roots certain transformed polynomials have in the interval $]0, 1[$. Finally, the isolating intervals for the roots of $p(x)$ are easily computed from the bijection

$$\alpha_{]0, ub[} = a + \alpha_{]0, 1[}(b - a) \quad (2)$$

which exists between the roots $\alpha_{]0, 1[} \in]0, 1[$ of the *transformed* polynomial $p(ub \cdot x)$ and the roots $\alpha_{]0, ub[} \in]a, b[=]0, ub[$ of the *original* polynomial $p(x)$.

The appropriate criterion mentioned above is a “*test*” that determines an *upper bound* on the number of positive roots in the interval $]0, 1[$.

Please observe that Descartes' rule of signs *cannot* be used in the interval $]0, 1[$, as it applies *only* to positive roots in the interval $]0, +\infty[$. Therefore, we have to resort to a different “*rule*” if we want to avoid reinventing Sturm's method for isolating the real roots; recall that Sturm's theorem gives us the *exact* number of positive roots in any interval $]a, b[$, see [20].

Here is a test for determining an *upper bound* on the number of positive roots in the interval $]0, 1[$: as explained below, it is named after Uspensky, who was the *first* to use it.

Uspensky's test. The number $\varrho_{01}(p)$ of real roots in the open interval $]0, 1[$ (multiplicities counted) of a polynomial $p(x) \in \mathbb{R}[x]$ is bounded above by $\text{var}_{01}(p)$, where

$$\text{var}_{01}(p) = \text{var} \left((x+1)^{\deg(p)} p\left(\frac{1}{x+1}\right) \right), \quad (3)$$

and we have $\text{var}_{01}(p) \geq \varrho_{01}(p)$.⁷

As in the case of Descartes' rule of signs, if $\text{var}_{01}(p) = 0$ it follows that $\varrho_{01}(p) = 0$, and if $\text{var}_{01}(p) = 1$ it follows that $\varrho_{01}(p) = 1$.

Therefore, Uspensky's test yields the *exact* number of positive roots *only* in the two special cases mentioned above; to wit, whenever $\text{var}_{01}(p) = 0$ or $\text{var}_{01}(p) = 1$.

Please note in Eq. (3) that, *after* the substitution $x \leftarrow \frac{1}{x+1}$, the positive roots of $p(x)$ that were in the interval $]0, 1[$ are now in $]0, +\infty[$, in which case Descartes' rule of signs *can* be applied.

Uspensky's test is associated with Budan's theorem [4] according to which for a given polynomial $p(x) \in \mathbb{Z}[x]$ the following two special cases hold:

- if $\text{var}(p(x)) = \text{var}(p(x+1))$, then we can conclude that there are no positive real roots of $p(x)$ in the interval $]0, 1[$,

and

- if $\text{var}(p(x)) - \text{var}(p(x+1)) = 1$, then we can conclude that there is one positive real root of $p(x)$ in the interval $]0, 1[$.

Vincent was fully aware of Budan's theorem, and, consequently, the substitution $x \leftarrow \frac{1}{x+1}$ is *never* used as a test in the VAS method (line 6 of Algorithm 1); it is performed *only* whenever $\text{var}(p(x)) - \text{var}(p(x+1)) \geq 2$, in which case the existence of positive roots in $]0, 1[$ *has* to be investigated. In other words, Vincent approaches a root as indicated in Fig. 5.

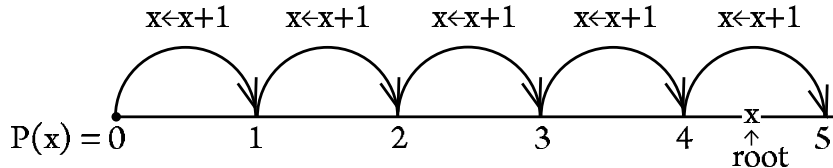


FIG. 5. Being aware of Budan's theorem, Vincent proceeded accordingly.

⁷Uspensky's test is a special case of the powerful “Vincent's test,” which is described below.

That, however, was not the case with Uspensky. Whenever he encountered $\text{var}(p(x)) = \text{var}(p(x+1))$ – not being aware of Budan’s theorem – he could not conclude that there are no positive roots of $p(x)$ in the interval $]0, 1[$; he could reach that conclusion *only* if $\text{var}_{01}(p) = 0$.⁸ Thus ([42, p. 128]), the transformation $x \leftarrow \frac{1}{1+x}$ was performed *before* the transformation $x \leftarrow x + 1$. In other words, Uspensky proceeded as indicated in Fig. 6.

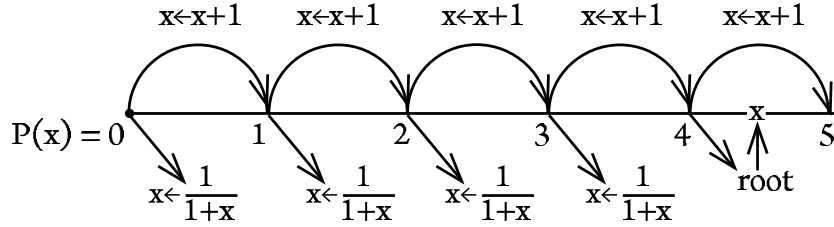


FIG. 6. Not being aware of Budan’s theorem, Uspensky proceeded making unnecessary transformations.

Therefore, Uspensky was the *first* to use $\text{var}_{01}(p) = 0$ *exclusively* as a test, in order to verify that there are no positive roots in the interval $]0, 1[$; hence, naming the test after him seems to be very appropriate. That test was used by Uspensky in his unsuccessful attempt to develop a new procedure for the isolation of the real roots of polynomials [5, 20].⁹

Below is a recursive description of the VCA bisection method:

THE VCA BISECTION METHOD, ORIGINAL VERSION

Input: A univariate, square-free polynomial $p(ub \cdot x) \in \mathbb{Z}[x]$, $p(0) \neq 0$, and the open interval $]a, b[=]0, ub[$, where ub is an upper bound on the values of the positive roots of $p(x)$. (The positive roots of $p(ub \cdot x)$ are all in the open interval $]0, 1[$.)

Output: A list of isolating intervals for the *positive* roots of $p(x)$.

```

1  var ← the number of sign changes of  $(x+1)^{\deg(p)} p(\frac{1}{x+1})$ ;
2  if var = 0 then RETURN  $\emptyset$ ;
3  if var = 1 then RETURN  $\{]a, b[ \}$ ;
4   $p_{0\frac{1}{2}} \leftarrow 2^{\deg(p)} p(\frac{x}{2})$  // Look for real roots in  $]0, \frac{1}{2}[$ ;
5   $m \leftarrow \frac{a+b}{2}$  // Is  $\frac{1}{2}$  a root?;
6   $p_{\frac{1}{2}1} \leftarrow 2^{\deg(p)} p(\frac{x+1}{2})$  // Look for real roots in  $] \frac{1}{2}, 1[$ ;
7  if  $p(\frac{1}{2}) \neq 0$  then
8    | RETURN  $\text{VCA}(p_{0\frac{1}{2}}, ]a, m[) \cup \text{VCA}(p_{\frac{1}{2}1}, ]m, b[)$ 
9  else
10   | RETURN  $\text{VCA}(p_{0\frac{1}{2}}, ]a, m[) \cup \{[m, m]\} \cup \text{VCA}(p_{\frac{1}{2}1}, ]m, b[)$ 
11 end
```

Algorithm 2. The *original* version of the $\text{VCA}(p,]a, b[$ “bisection” algorithm, where the second argument is the open interval $]a, b[$ associated with $p(x)$. The isolating intervals for the roots of $p(x)$ are computed directly, without using the bijection (2).

The VCA bisection method has been implemented in the computer algebra system *Maple*, where it can be used *after* loading an appropriate package; see Fig. 7. Please note that the VCA bisection method uses Uspensky’s test

⁸On the other hand, Uspensky used correctly, and to his advantage, the other special case, $\text{var}_{01}(p) = 1$, as well as the case $\text{var}_{01}(p) \geq 2$.

⁹According to Professor Alexei Uteshev [43], of the St.Petersburg State University, the reason for Uspensky’s unsuccessful attempt was the fact that he *never* saw Vincent’s actual paper of 1836, where Budan’s theorem is stated right at the beginning. Instead, Uspensky relied on the Russian translation of J.-A. Serret’s *Cours d’Algèbre Supérieure* [35]. Indeed, in Sec. 167, p. 315, we read: “В одном из мемуаров, составляющих часть первого тома Journal de Mathématiques Pures et Appliquées, Винсент изложил прекрасное свойство непрерывных дробей и вывел из него для вычисления вещественных корней уравнения способ, вытекающий одновременно и из способа Ньютона, и из способа Лагранжа...” Please note that Serret presents *Fourier’s* theorem under the name “Budan.”

as a termination criterion (lines 1–3) and that the upper bound on the values of the positive roots is computed *only* once. An excellent discussion of this algorithm can be found in [24]; another version of the same algorithm as well as additional information can be found elsewhere, see [7].

```

> with(RootFinding) :
> f := x300 - 2(5 x - 1)2;
                                     f := x300 - 2 (5 x - 1)2
> st := time( ) : Isolate(f, digits = 250) : time( ) - st,
                                     170.431
>

```

FIG. 7. For the Mignotte polynomials, the VCA bisection method is several thousand times slower than the VAS continued fractions method (see also Fig. 4).

Moreover, note the following:

- The substitutions in lines 4 and 6 are performed only on the polynomial $p(x)$, whereas at the same time – in line 5 – the interval $]a, b[$ is divided into two equal parts $]a, m[$ and $]m, b[$, to be used in line 8 or 10.
- To isolate the real roots of $p(x)$ in the open interval $]0, 1[$, we proceed as follows:
 - we first isolate the real roots in the interval $]0, \frac{1}{2}[$ (lines 4 and 8 or 10),
 - we then deal with the case where $\frac{1}{2}$ is a root of $p(x)$ (lines 5, 7, and 10),
 - and, finally, we isolate the real roots in the interval $]\frac{1}{2}, 1[$ (lines 6 and 8 or 10).
- The isolating intervals are directly obtained from line 3 – except for those roots that happen to coincide with the midpoint of an interval that gets bisected, in which case they are computed in lines 5 and 10.

The computing time of the VCA bisection method is

$$O(n^4 \tau^2),$$

where n is the degree of the polynomial and τ bounds the coefficient bitsize, see [37].

The *second* bisection method was developed by Alesina and Galuzzi [20, 22] in 2000. It uses Vincent’s powerful test as a termination criterion and bisects the interval $]a, b[=]0, ub[$, where ub is an upper bound on the values of the positive roots. Therefore, this method is a direct implementation of Theorem 2.

Vincent’s test. If $a \geq 0$ and $b > a$, then the number $\varrho_{ab}(p)$ of real roots in the open interval $]a, b[$ (multiplicities counted) of the polynomial $p(x) \in \mathbb{R}[x]$ is bounded above by $\text{var}_{ab}(p)$, where

$$\text{var}_{ab}(p) = \text{var} \left((1+x)^{\deg(p)} p\left(\frac{a+bx}{1+x}\right) \right), \quad (4)$$

and we have $\text{var}_{ab}(p) = \text{var}_{ba}(p) \geq \varrho_{ab}(p)$.

Note that this test can be applied also in the case $]a, b[=]1, 0[$, from which we obtain Uspensky’s test.¹⁰

As in the case of Descartes’ rule of signs, if $\text{var}_{ab}(p) = 0$ it follows that $\varrho_{ab}(p) = 0$, and if $\text{var}_{ab}(p) = 1$ it follows that $\varrho_{ab}(p) = 1$.

Therefore, Vincent’s test yields the *exact* number of positive roots *only* in the two special cases mentioned above; to wit, whenever $\text{var}_{ab}(p) = 0$ or $\text{var}_{ab}(p) = 1$.

Below is a recursive description of the second bisection method derived from Vincent’s theorem; its simplicity is unsurpassed, but we pay for it by using a much more complicated test. Obviously, there is a trade-off between the simplicity of the method and the complexity of the termination test.

Please note the following:

- Vincent’s test is a *crucial component* of the $B(p,]a, b[)$ bisection algorithm (lines 1–3).

¹⁰By comparison, Uspensky’s test is rather weak, as it applies *only* in the interval $]a, b[=]0, 1[$.

- In line 4 the interval $]a, b[$ is divided into two equal parts $]a, m[$ and $]m, b[$, to be used in lines 6 or 8. Note that there are no polynomial transformations at all; only polynomial evaluations in line 1.
- To isolate the real roots of $p(x)$ in the open interval $]a, b[$, we proceed as follows:
 - we first isolate the real roots in the interval $]a, \frac{a+b}{2}[$ (lines 6 or 8),
 - we then deal with the case where $\frac{a+b}{2}$ is a root of $p(x)$ (lines 5 and 8),
 - and, finally, we isolate the real roots in the interval $]\frac{a+b}{2}, b[$ (lines 6 or 8).
- The isolating intervals are directly obtained from line 3 – except for those roots that happen to coincide with the midpoint of an interval that gets bisected, in which case they are computed in lines 5 and 8.

THE VINCENT–ALESINA–GALUZZI BISECTION METHOD: B

<p>Input: A univariate, square-free polynomial $p(x) \in \mathbb{Z}[x]$, $p(0) \neq 0$, and the open interval $]a, b[=]0, ub[$, where ub is an upper bound on the values of the positive roots of $p(x)$.</p> <p>Output: A list of isolating intervals for the <i>positive</i> roots of $p(x)$.</p> <pre> 1 var ← the number of sign changes of $(1+x)^{\deg(p)}p(\frac{a+bx}{1+x})$; 2 if var = 0 then RETURN \emptyset; 3 if var = 1 then RETURN $\{]a, b[\}$; 4 $m \leftarrow \frac{a+b}{2}$ //Subdivide the interval $]a, b[$ into two equal parts; 5 if $p(m) \neq 0$ then 6 RETURN $(B)(p,]m[) \cup (B)(p,]m, b[)$ 7 else 8 RETURN $(B)(p,]m[) \cup \{[m, m]\} \cup (B)(p,]m, b[)$ 9 end</pre>

Algorithm 3. The $B(p,]a, b[)$ “*bisection*” algorithm, proposed by Alesina and Galuzzi [22]; the second argument is the open interval $]a, b[$, whose endpoints a, b are used in Vincent’s test in line 1. The isolating intervals for the roots of $p(x)$ are computed directly, without using the bijection (2).

A complete discussion and empirical comparison between the two bisection methods can be found elsewhere, see [18]. It turns out that the Vincent–Alesina–Galuzzi bisection method, despite its simplicity, is much slower than the VCA bisection method and hence of little practical importance.

4. IMPROVING THE PERFORMANCE OF THE VAS CONTINUED FRACTIONS METHOD

As was pointed out in the discussion of VAS, the efficiency of this continued fractions method depends heavily on how good the estimates of the lower bounds on the values of the positive roots are.

A *lower* bound, ℓb , on the values of the positive roots of a polynomial $p(x)$ of degree n is found by first computing an *upper* bound, ub , on the values of the positive roots of $x^n p(\frac{1}{x})$ and then setting $\ell b = \frac{1}{ub}$.

So, clearly, what is needed is an efficient method for computing upper bounds on the values of (just) the positive roots of polynomial equations.

In the initial implementation of VAS, in 1978, the lower bounds were computed using a theorem by Cauchy, see [32]. To state it, we refer to polynomials of the type

$$p(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_0 \quad (\alpha_n > 0) \quad (5)$$

with real coefficients $\alpha_n, \alpha_{n-1}, \dots, \alpha_0$ having at least one sign variation.

Theorem 4 (Cauchy’s theorem). *Let $p(x)$ be a polynomial as in Eq. (5), of degree $n > 0$, with $\alpha_{n-k} < 0$ for at least one k , $1 \leq k \leq n$. If λ is the number of negative coefficients, then an upper bound on the values of the positive roots of $p(x)$ is given by*

$$ub_C = \max_{\{1 \leq k \leq n: \alpha_{n-k} < 0\}} \sqrt[k]{-\frac{\lambda \alpha_{n-k}}{\alpha_n}}.$$

Note that if $\lambda = 0$, then there are no positive roots.

Subsequently, Kioustelidis’ bound appeared (in [30]), and was used in the SYNAPS implementation of VAS by Tsigaridas and Emiris [41] in 2006. Kioustelidis’ theorem is closely related to Cauchy’s one and is stated below.

Theorem 5 (Kioustelidis’ theorem). *Let $p(x)$ be a polynomial as in Eq. (5), of degree $n > 0$, with $\alpha_{n-k} < 0$ for at least one k , $1 \leq k \leq n$. Then an upper bound on the values of the positive roots of $p(x)$ is given by*

$$ub_K = 2 \max_{\{1 \leq k \leq n: \alpha_{n-k} < 0\}} \sqrt[k]{-\frac{\alpha_{n-k}}{\alpha_n}}.$$

However, both implementations of the VAS continued fractions method – that is, using either Cauchy’s or Kioustelidis’ bound – showed that its “Achilles’ heel” was the case of very many very large rational roots. In this case, the VAS method was up to 4 times slower than VCA(rl) – the fastest implementation of the VCA bisection method developed by Rouillier and Zimmermann [34]. Table 1 presented below corresponds to the last table (Table 4) found in [14].

Roots (bit length)	Degree	No. of roots	VAS $t(s)/M(MB)$	VCA(rl) $t(s)/M(MB)$
10	100	100	0.8/1.82	0.61/1.92
10	200	200	2.45/2.07	10.1/2.64
10	500	500	33.9/3.34	878/8.4
1000	20	20	0.12/1.88	0.044/1.83
1000	50	50	16.7/3.18	4.27/2.86
1000	100	100	550/8.9	133/6.49

TABLE 1. Products of factors (x -randomly generated integer roots). All computations were done on a 850 MHz Athlon PC with 256 MB RAM; (s) stands for time in seconds, and (MB) for the amount of memory used in MBytes.

The last three lines of Table 1 demonstrate the weaker performance of VAS in the case of very many very large rational roots.

Therefore, the question was posed: can we improve the performance of VAS by discovering new bounds on the values of the positive roots?

In order to answer this question, we needed to better understand the nature of these bounds, and this was achieved with the help of Ștefănescu’s theorem [38] of 2005.

Theorem 6 (Ștefănescu’s theorem, 2005). *Let $p(x) \in R[x]$ be a polynomial such that the number of variations of signs of its coefficients is **even**. If*

$$p(x) = c_1 x^{d_1} - b_1 x^{m_1} + c_2 x^{d_2} - b_2 x^{m_2} + \dots + c_k x^{d_k} - b_k x^{m_k} + g(x),$$

with $g(x) \in R_+[x]$, $c_i > 0$, $b_i > 0$, $d_i > m_i > d_{i+1}$ for all i , then the number

$$ub_S = \max \left\{ \left(\frac{b_1}{c_1} \right)^{1/(d_1-m_1)}, \dots, \left(\frac{b_k}{c_k} \right)^{1/(d_k-m_k)} \right\}$$

*is an upper bound for the positive roots of the polynomial p for any **choice** of c_1, \dots, c_k .*

Ștefănescu’s theorem introduces the concept of *matching* or *pairing* a positive coefficient with an unmatched negative coefficient of a lower order term; however, Ștefănescu’s theorem worked *only* for polynomials with an even number of sign variations.

Note. More precisely, it is the *term* with a positive coefficient that is being matched to the *term* with a negative coefficient.

We generalized Ștefănescu’s theorem, in the sense that Theorem 7 below applies to polynomials with any number of sign variations, see [15]. To accomplish this, we introduced the concept of *breaking up* a positive coefficient into several parts to be paired with negative coefficients of lower order terms,¹¹ see [16].

¹¹After our work [16], Ștefănescu also extended his Theorem 6 in [39].

Theorem 7 (Akritas–Strzeboński–Vigklas, 2006). *Let*

$$p(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_0 \quad (\alpha_n > 0)$$

be a polynomial with real coefficients, and let $d(p)$ and $t(p)$ denote its degree and the number of its terms, respectively.

Moreover, assume that $p(x)$ can be written as

$$p(x) = q_1(x) - q_2(x) + q_3(x) - q_4(x) + \cdots + q_{2m-1}(x) - q_{2m}(x) + g(x), \quad (6)$$

where all the polynomials $q_i(x)$, $i = 1, 2, \dots, 2m$, and $g(x)$ have only positive coefficients. In addition, assume that for $i = 1, 2, \dots, m$ we have

$$q_{2i-1}(x) = c_{2i-1,1} x^{e_{2i-1,1}} + \cdots + c_{2i-1,t(q_{2i-1})} x^{e_{2i-1,t(q_{2i-1})}}$$

and

$$q_{2i}(x) = b_{2i,1} x^{e_{2i,1}} + \cdots + b_{2i,t(q_{2i})} x^{e_{2i,t(q_{2i})}},$$

where $e_{2i-1,1} = d(q_{2i-1})$ and $e_{2i,1} = d(q_{2i})$, and the exponent of each term in $q_{2i-1}(x)$ is greater than the exponent of each term in $q_{2i}(x)$. If for all indices $i = 1, 2, \dots, m$, we have

$$t(q_{2i-1}) \geq t(q_{2i}),$$

then an upper bound on the values of the positive roots of $p(x)$ is given by

$$ub = \max_{\{i=1,2,\dots,m\}} \left\{ \left(\frac{b_{2i,1}}{c_{2i-1,1}} \right)^{\frac{1}{e_{2i-1,1} - e_{2i,1}}}, \dots, \left(\frac{b_{2i,t(q_{2i})}}{c_{2i-1,t(q_{2i})}} \right)^{\frac{1}{e_{2i-1,t(q_{2i})} - e_{2i,t(q_{2i})}}} \right\}, \quad (7)$$

for any permutation of the positive coefficients $c_{2i-1,j}$, $j = 1, 2, \dots, t(q_{2i-1})$. Otherwise, for each of the indices i for which we have

$$t(q_{2i-1}) < t(q_{2i}),$$

*we **break up** one of the coefficients of $q_{2i-1}(x)$ into $t(q_{2i}) - t(q_{2i-1}) + 1$ parts, so that now $t(q_{2i}) = t(q_{2i-1})$, and apply the same formula (7) given above.*

For a proof of this theorem, see [16]. Please note that the partial extension of Theorem 6 presented in [15] does not treat the case $t(q_{2i-1}) < t(q_{2i})$.

Crucial observation 2. Pairing up positive with negative coefficients and breaking up a positive coefficient into a required number of parts – to match the corresponding number of negative coefficients – are the key ideas of this theorem. In general, formulas analogous to (7) hold for the cases where: (a) we pair coefficients from nonadjacent polynomials $q_{2l-1}(x)$ and $q_{2i}(x)$, for $1 \leq l < i$, and (b) we break up one or more positive coefficients into several parts to be paired with negative coefficients of lower order terms.

Using Theorem 7, we obtain the following interpretation of Cauchy’s and Kioustelidis’ theorems:

- C** Cauchy’s “leading-coefficient” implementation of Theorem 7. For a polynomial $p(x)$ as in Eq. (5) with λ negative coefficients, the Cauchy method first breaks up its leading coefficient α_n into λ *equal* parts and then pairs each part with the first unmatched negative coefficient.
- K** Kioustelidis’ “leading-coefficient” implementation of Theorem 7. For a polynomial $p(x)$ as in Eq. (5), the Kioustelidis method matches the coefficient $-\alpha_{n-k}$ of the term $-\alpha_{n-k} x^{n-k}$ in $p(x)$ with $\frac{\alpha_n}{2^k}$, the leading coefficient divided by 2^k .

Kioustelidis’ “leading-coefficient” implementation of Theorem 7 differs from that of Cauchy only in that the leading coefficient is now broken up into *unequal* parts, since we divide it by different powers of 2.

It turns out that all methods for computing upper bounds on the values of the positive roots of a polynomial are derived from Theorem 7. In what follows, we present linear and quadratic complexity bounds derived from Theorem 7 and elaborate on their impact on the efficiency of VAS.

4.1. Improving VAS with linear complexity bounds derived from Theorem 7

The bounds in the literature, such as Cauchy's and Kioustelidis' ones, are of *linear* complexity.

The general idea of linear complexity bounds. These bounds are computed as follows:

- *each* negative coefficient of the polynomial is paired with *one* of the preceding *unmatched* positive coefficients;
- the maximum of all the computed radicals is taken as the estimate of the bound.

Using Theorem 7, we developed *first-λ*, a new linear complexity method for computing an upper bound on the values of the positive roots of polynomials.

FL The “**first-λ**” implementation of Theorem 7. For a polynomial $p(x)$ as in (6) with λ negative coefficients, we first take care of all cases for which $t(q_{2i}) > t(q_{2i-1})$, by breaking up the last coefficient $c_{2i-1, t(q_{2i})}$ of $q_{2i-1}(x)$ into $t(q_{2i}) - t(q_{2i-1}) + 1$ *equal* parts. We then pair each of the first λ positive coefficients of $p(x)$, encountered as we move in nonincreasing order of exponents, with the first unmatched negative coefficient.

This is an improvement over the other two bounds due to Cauchy and Kioustelidis, but, as the following example demonstrates, all three methods can fail miserably.

Example 2. Consider the polynomial

$$x^3 + 10^{100}x^2 - 10^{100}x - 1,$$

which has one sign variation and hence only one positive root equal to 1.

- For Cauchy's theorem, we pair the terms $\{\frac{x^3}{2}, -10^{100}x\}$ and $\{\frac{x^3}{2}, -1\}$, and obtain the bound of $1.41421 * 10^{50}$.
- For Kioustelidis' theorem, we pair the terms $\{\frac{x^3}{2^2}, -10^{100}x\}$ and $\{\frac{x^3}{2^2}, -1\}$, and obtain the bound of $2 * 10^{50}$.
- For *first-λ*, we pair the terms $\{x^3, -10^{100}x\}$ and $\{10^{100}x^2, -1\}$, and obtain the bound of 10^{50} .

To correct this inadequacy, we developed *local-max*, yet another new linear complexity method for computing an upper bound on the values of the positive roots of polynomials.

LM The “**local-max**” implementation of Theorem 7. For a polynomial $p(x)$ as in (5), the coefficient $-\alpha_k$ of the term $-\alpha_k x^k$ in $p(x)$ – as given in Eq. (5) – is paired with the coefficient $\frac{\alpha_m}{2^t}$, of the term $\alpha_m x^m$, where α_m is the largest positive coefficient with $n \geq m > k$ and t indicates the number of times the coefficient α_m has been used.

Example 2, continued. For *local-max*, we pair the terms

$$\left\{ \frac{10^{100}x^2}{2}, -10^{100}x \right\} \quad \text{and} \quad \left\{ \frac{10^{100}x^2}{2^2}, -1 \right\},$$

and obtain the bound of 2.

We have tested extensively – on various classes of specific and random polynomials – all four linear complexity bounds mentioned above, and the following is a summary of our findings, see [16]:

- Kioustelidis' bound is, in general, better (or much better) than Cauchy's one; this happens because the former breaks up the leading coefficient into *unequal* parts, whereas the latter breaks it up into *equal* parts.
- Our *first-λ* bound, as the name indicates, uses additional coefficients, and, therefore, it is not surprising that it is, in general, better (or much better) than both previous bounds. In the few cases where Kioustelidis' bound is better than *first-λ*, our *local-max* bound takes the lead again.

Therefore, given their linear execution cost, $\min(FL, LM)$ or $FL + LM$ is the best among the linear complexity bounds on the values of the positive roots of a polynomial, see [16].

In Table 2 below we recalculate the results of Table 1 and compare the timings in seconds, $t(s)$, for (a) VAS(Cauchy), the VAS continued fractions method using Cauchy's rule (the “*old*” method), (b) VAS(f1+1m), the VAS continued fractions method using $\min(FL, LM)$ or $FL + LM$ (the “*new*” method), and (c) VCA(rel), the fastest implementation of the VCA bisection method. (Table 2 corresponds to the last table (Table 2) found in [17].)

Roots	Deg	VAS(Cauchy) $t(s)$ Average (Min/Max)	VAS(f1+1m) $t(s)$ Average (Min/Max)
10	100	0.314(0.248/0.392)	0.253(0.228/0.280)
10	200	1.74(1.42/2.33)	1.51(1.34/1.66)
10	500	17.6(16.9/18.7)	17.4(16.3/18.1)
000	20	0.066(0.040/0.084)	0.031(0.024/0.040)
1000	50	1.96(1.45/2.44)	0.633(0.512/0.840)
1000	100	52.3(36.7/81.3)	12.7(11.3/14.6)
Roots	Deg	VCA(rl) $t(s)$ Average (Min/Max)	Memory (MB) old/new/rel
10	110	0.346(0.308/0.384)	4.46/4.48/4.56
10	200	3.90(3.72/4.05)	4.73/4.77/5.35
10	500	129(122/140)	6.28/6.54/11.8
000	20	0.038(0.028/0.044)	4.57/4.62/4.51
1000	50	1.03(0.916/1.27)	5.87/6.50/5.55
1000	100	17.2(16.1/18.7)	10.4/11.7/9.17

TABLE 2. Products of the terms $x - r$ with a random integer r . The tests were run on a laptop computer with 1.8 Ghz Pentium M processor, running a Linux virtual machine with 1.78 GB of RAM.

Due to different computational environments, the times $t(s)$ differ substantially, but they confirm the fact that VAS(f1+1m) is now *always* faster than VCA(rl).

Again, it is interesting to look at the last three lines of Table 2, where, as in Table 1, the performance of VAS(Cauchy) is worse than that of VCA(rl) – at worst 3 times slower, as the last entry indicates. However, from these same lines of Table 2 we observe that VAS(f1+1m) is now always faster than VCA(rl) – at best twice as fast, as can be seen in the 5th line.

When we compare – on various classes of specific and random polynomials – the times of VAS(Cauchy) with those of VAS(f1+1m), we observe an overall speed-up of 15%, see [19].

4.2. Improving VAS with quadratic complexity bounds derived from Theorem 7

To further improve the performance of the VAS continued fractions method, we decided to use quadratic complexity bounds on the values of the positive real roots, hoping that their improved estimates *should* compensate for the extra time needed to compute them.

The general idea of quadratic complexity bounds. These bounds are computed as follows:

- *each* negative coefficient of the polynomial is paired with *all* the preceding positive coefficients, and the minimum of the computed values is taken;
- the maximum of all those minimums is taken as the estimate of the bound.

In general, the estimates obtained from quadratic complexity bounds are better than those obtained from the corresponding linear complexity bounds, as the former are computed with much more effort and time.¹²

We developed several new quadratic complexity bounds by extending three (of the four) linear complexity ones, see [8]; by contrast, Kioustelidis’ linear complexity bound was extended by Hong [28] in 1998. We were able to demonstrate that one of them, *FLQ*, the “first- λ ” quadratic complexity bound, is not only one of the best to be used in VAS, but also the fastest, see [9]. However, we decided that the following quadratic complexity bound should be used in VAS instead, see [19].

LMQ The “local-max” quadratic complexity implementation of Theorem 7. For a polynomial $p(x)$ as in (5), each negative coefficient $a_i < 0$ is “paired” with *each* of the preceding positive coefficients a_j divided by 2^{t_j} ; that is, *each* positive coefficient a_j is “broken up” into *unequal* parts, as is done with *just* the locally maximal coefficient in the local-max bound; t_j is initially set to 1 and is incremented each time the positive coefficient a_j is used; and the minimum is taken over all j ; subsequently, the maximum is taken over all i .

¹²It should be noted that time is not so important in our case, since – as can be seen from the description of the VAS algorithm, line 4, – these bounds are estimated *before* a translation of complexity at *least* $O(n^2)$ is executed, see [29].

That is, we have

$$ub_{\text{LMQ}} = \max_{\{a_i < 0\}} \min_{\{a_j > 0: j > i\}} \sqrt[j-i]{-\frac{a_i}{\frac{a_j}{2^{t_j}}}}.$$

Today LMQ is theoretically the sharpest bound on the values of the positive roots of a polynomial, and using it in VAS has resulted in an overall speed-up of 40% over its initial implementation.

We finally present Table 3 – corresponding to Table 8 in [19] – where we demonstrate the performance of VAS using quadratic complexity bounds. This is actually the only case where the best linear complexity bound $FL + LM$ is slightly better than LMQ.

Bit-length of roots	Degree	VAS(Cauchy) $t(s)$ Avg(Min/Max)	VAS(fl+lm) $t(s)$ Avg(Min/Max)	VAS(lmq) $t(s)$ Avg(Min/Max)
10	100	0.46(0.28/0.94)	0.24(0.18/0.28)	0.34(0.30/0.41)
10	200	1.46(1.24/1.85)	1.40(1.28/1.69)	1.40(1.20/1.69)
10	500	18.1(16.5/18.9)	18.1(16.6/18.8)	22.1(18.7/24.2)
1000	20	0.07(0.04/0.14)	0.02(0.02/0.03)	0.03(0.02/0.04)
1000	50	3.69(2.38/6.26)	0.81(0.60/1.28)	0.81(0.52/1.11)
1000	100	47.8(37.6/56.9)	13.8(10.3/19.2)	15.8(11.3/21.3)

TABLE 3. Products of the terms $x - r$ with random integer r . The average speed-up for this table is about 35%.

5. CONCLUSION

We have presented Vincent’s theorem of 1836, along with various methods derived from it for isolating the real roots of polynomials with rational coefficients. It was shown that the VAS continued fractions method has always been the fastest, and recently – with the development of quadratic complexity bounds – its performance has increased by an overall factor of 40%.

We end our presentation with a list of topics for future research:

- Sharma’s bound on the computing time of the VAS continued fractions method is *greatly overestimated*. Hence, theoretical research is needed to see if we can bring it down.
- The VAS continued fractions method works for *integer* or *rational* coefficients. Hence, we need to discover new ways to deal with coefficients that are *algebraic* numbers or *approximate* reals.
- The VAS continued fractions method is the fastest real root isolation method when the polynomials are *not* sparse and their degree is less than a few thousand. However, *Mathematica runs out of memory* when we try to isolate the roots of a sparse polynomial of degree 100000 or greater. Hence, we need to discover new ways to deal with sparse polynomials of extremely high degrees.
- Last, but not least, we need to investigate the performance of the VAS continued fractions method in a multiprocessor environment.

This paper is based on the *plenary talk* the author gave at ACA 2008, the International Conference on Applications of Computer Algebra, held at RISC-Linz, Hagenberg, Austria (July 27–30, 2008).

REFERENCES

1. A. G. Akritas, “Vincent’s theorem in algebraic manipulation,” Ph.D. thesis, North Carolina State University, Raleigh (1978).
2. A. G. Akritas, “An implementation of Vincent’s Theorem,” *Numer. Math.*, **36**, 53–62 (1980).
3. A. G. Akritas, “The fastest exact algorithms for the isolation of the real roots of a polynomial equation,” *Computing*, **24**, 299–313 (1980).
4. A. G. Akritas, “Reflections on a pair of theorems by Budan and Fourier,” *Math. Mag.*, **55**, No. 5, 292–298 (1982).
5. A. G. Akritas, “There is no ‘Uspensky’s method’,” in: *Proceedings of the 1986 Symposium on Symbolic and Algebraic Computation*, Waterloo, Ontario, Canada (1986), pp. 88–90.
6. A. G. Akritas, *Elements of Computer Algebra with Applications*, John Wiley Interscience, New York (1989).

7. A. G. Akritas, "There is no 'Descartes' method'," in: M. J. Wester and M. Beaudin (eds.), *Computer Algebra in Education*, Aulona Press, White Lake (2008), pp. 19–35.
8. A. G. Akritas, "Linear and quadratic complexity bounds on the values of the positive roots of polynomials," submitted.
9. A. G. Akritas, A. I. Argyris, and A. W. Strzeboński, "FLQ, the fastest quadratic complexity bound on the values of positive roots of polynomials," *Serdica J. Comput.*, **2**, 145–162 (2008).
10. A. G. Akritas, A. Bocharov, and A. W. Strzeboński, "Implementation of real root isolation algorithms in *Mathematica*," in: *Abstracts of the International Conference on Interval and Computer-Algebraic Methods in Science and Engineering* (Interval '94), St. Petersburg, Russia (1994), pp. 23–27.
11. A. G. Akritas and S. D. Danielopoulos, "On the forgotten theorem of Mr. Vincent," *Historia Math.*, **5**, 427–435 (1978).
12. A. G. Akritas and S. D. Danielopoulos, "An unknown theorem for the isolation of the roots of polynomials," *Ganita-Bharati (Bulletin of the Indian Society for History of Mathematics)*, **2**, 41–49 (1980).
13. A. G. Akritas and K. H. Ng, "Exact algorithms for polynomial real root approximation using continued fractions," *Computing*, **30**, 63–76 (1983).
14. A. G. Akritas and A. Strzeboński, "A comparative study of two real root isolation methods," *Nonlinear Anal. Model. Control*, **10**, No. 4, 297–304 (2005).
15. A. G. Akritas and P. Vigklas, "A comparison of various methods for computing bounds for positive roots of polynomials," *J. Univ. Comput. Sci.*, **13**, No. 4, 455–467 (2007).
16. A. G. Akritas, A. Strzeboński, and P. Vigklas, "Implementations of a new theorem for computing bounds for positive roots of polynomials," *Computing*, **78**, 355–367 (2006).
17. A. G. Akritas, A. Strzeboński, and P. Vigklas, "Advances on the continued fractions method using better estimations of positive root bounds," in: V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov (eds.), *Proceedings of the 10th International Workshop on Computer Algebra in Scientific Computing (CASC)*, Bonn, September 16–20, 2007, *Lect. Notes Comput. Sci.*, **4770**, Springer-Verlag, Berlin (2007), pp. 24–30.
18. A. G. Akritas, A. Strzeboński, and P. Vigklas, "On the various bisection methods derived from Vincent's theorem," *Serdica J. Comput.*, **2**, 89–104 (2008).
19. A. G. Akritas, A. Strzeboński, and P. Vigklas, "Improving the performance of the continued fractions method using new bounds of positive roots," *Nonlinear Anal. Model. Control* **13**, No. 3, 265–279 (2008).
20. A. Alesina and M. Galuzzi, "A new proof of Vincent's theorem," *Enseign. Math.*, **44**, 219–256 (1998).
21. A. Alesina and M. Galuzzi, "Addendum to the paper 'A new proof of Vincent's theorem'," *Enseign. Math.*, **45**, 379–380 (1999).
22. A. Alesina and M. Galuzzi, "Vincent's theorem from a modern point of view," in: R. Betti and W. F. Lawvere (eds.), *Categorical Studies in Italy* (Perugia, 1997), *Rend. Circ. Mat. Palermo, Serie II*, **64** (2000), pp. 179–191.
23. E. Bombieri and A. J. van der Poorten, "Continued fractions of algebraic numbers," in: *Computational Algebra and Number Theory* (Sydney, 1992), *Math. Appl.*, **325**, Kluwer Academic Publishers, Dordrecht (1995), pp. 137–152.
24. F. Boulier, "Systèmes polynomiaux: que signifie "résoudre"?", Lecture notes, Université Lille 1 (2007); <http://www2.lifl.fr/~boulier/RESOUDRE/SHARED/support.pdf>; <http://www.fil.univ-lille1.fr/portail/ls4/resoudre>.
25. F. Boulier, Private communication, October 2007.
26. D. G. Cantor, P. H. Galyean, and H. G. Zimmer, "A continued fraction algorithm for real algebraic numbers," *Math. Comput.*, **26**, No. 119, 785–791 (1972).
27. G. E. Collins and A. G. Akritas, "Polynomial real root isolation using Descartes' rule of signs," in: *Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computations*, Yorktown Heights, New York (1976), pp. 272–275.
28. H. Hong, "Bounds for absolute positiveness of multivariate polynomials," *J. Symbolic Comput.*, **25**, No. 5, 785–791 (1998).
29. J. von zur Gathen and J. Gerhard, "Fast algorithms for Taylor shifts and certain difference equations," in: *Proceedings of ISSAC'97*, Maui, Hawaii (1997), pp. 40–47.
30. B. Kioustelidis, "Bounds for positive roots of polynomials," *J. Comput. Appl. Math.*, **16**, No. 2, 241–244 (1986).
31. E. K. Lloyd, "On the forgotten Mr. Vincent," *Historia Math.*, **6**, 448–450 (1979).

32. N. Obreschkoff, *Verteilung und Berechnung der Nullstellen reeller Polynome*, VEB Deutscher Verlag der Wissenschaften, Berlin (1963).¹³
33. A. M. Ostrowski, "Note on Vincent's theorem," *Ann. Math.*, Ser 2., **52**, No. 3, 702–707 (1950).
34. F. Rouillier and P. Zimmermann, "Efficient isolation of polynomial's real roots," *J. Comput. Appl. Math.*, **162**, 33–50 (2004).
35. J.-A. Serret, *Cours d'Algèbre Supérieure*, Vol. 1, 2, Gauthier–Villars, Paris (1866). Copies of these volumes can be downloaded from <http://www.archive.org/details/coursdalgebsuper01serrrich>.
36. V. Sharma, "Complexity of real root isolation using continued fractions," ISAAC'07 Preprint (2007).
37. V. Sharma, "Complexity analysis of algorithms in algebraic computation," Ph.D. thesis, Department of Computer Science, Courant Institute of Mathematical Science, New York University (2007).
38. D. Ștefănescu, "New bounds for positive roots of polynomials," *J. Univ. Comput. Sci.*, **11**, No. 12, 2132–2141 (2005).
39. D. Ștefănescu, "Bounds for real roots and applications to orthogonal polynomials," in: V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov (eds.), *Proceedings of the 10th International Workshop on Computer Algebra in Scientific Computing* (CASC 2007), Bonn, September 16–20, 2007, *Lect. Notes Comput. Sci.*, **4770**, Springer-Verlag, Berlin–Heidelberg (2007), pp. 377–391.
40. K. Thull, "Approximation by continued fraction of a polynomial real root," in: *Proceedings of the 1984 ACM Symposium on Symbolic and Algebraic Computations*, *Lect. Notes Comput. Sci.*, **174** (1984), pp. 367–377.
41. E. P. Tsigaridas and I. Z. Emiris, "Univariate polynomial real root isolation: Continued fractions revisited," in: Y. Azar and T. Erlebach (eds.), *Proceedings of the ESA 2006*, *Lect. Notes Comput. Sci.*, **4168** (2006), pp. 817–828.
42. J. V. Uspensky, *Theory of Equations*, McGraw-Hill, New York (1948).
43. A. Yu. Uteshev, Private communication, September 2007.
44. A. J. H. Vincent, "Sur la resolution des équations numériques," *Journal de Mathématiques Pures et Appliquées*, **1**, 341–372 (1836).
45. C. K. Yap, *Fundamental Problems of Algorithmic Algebra*, Oxford Univ. Press, New York (2000).

¹³For an English translation of a book with similar content, see: N. Obreschkoff, *Zeros of Polynomials*, Bulgarian Academic Monographs, **7**, Sofia (2003).