Journal of Symbolic Computation 79 (2017) 444–456

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

On the maximum computing time of the bisection method for real root isolation

George E. Collins

ARTICLE INFO

Article history:
Received 16 November 2014
Accepted 27 February 2016
Available online 2 March 2016

Keywords:
Polynomial roots
Real roots
Root isolation
Computing time
Algorithm analysis
Dominance

ABSTRACT

The bisection method for polynomial real root isolation was introduced by Collins and Akritas in 1976. In 1981 Mignotte introduced the polynomials $A_{a,n}(x) = x^n - 2(ax-1)^2$, a an integer, $a \geq 2$ and $n \geq 3$. First we prove that if a is odd then the computing time of the bisection method when applied to $A_{a,n}$ dominates $n^5(\log d)^2$ where d is the maximum norm of $A_{a,n}$. Then we prove that if A is any polynomial of degree n with maximum norm d then the computing time of the bisection method, with a minor improvement regarding homothetic transformations, is dominated by $n^5(\log d)^2$. It follows that the maximum computing time of the bisection method is codominant with $n^5(\log d)^2$.

1. Introduction

We adopt the terminology "bisection method" for the polynomial real root isolation method introduced in Collins and Akritas (1976). In this paper we prove that when the method (using classical arithmetic for polynomial translations) is applied to the Mignotte polynomials (Mignotte, 1981), $A_{a,n}(x) = x^n - 2(ax-1)^2$ with a an odd integer, $a \geq 3$ and $n \geq 3$, its computing time dominates $n^5(\log d)^2$, where d is the max norm, $4a^2$, of $A_{a,n}$. (A quite similar result concerning the continued fractions method was recently proved in Collins (2016).)

In Section 2 we prove important theorems about the real and complex roots of $A_{a,n}$. In Section 3 we introduce notation to be used for polynomial transformations. In Section 4 we define a binary tree associated with the transformations performed on $A_{a,n}$, estimate its height, and show that it is isomorphic to a finite portion of the tree for computing the decimal expansion of $1/a$. In Section 5 we analyze the transformed polynomials, obtaining formulas for their coefficients. In Sections 6 and

E-mail address: gcollins8@charter.net.

http://dx.doi.org/10.1016/j.jsc.2016.02.017

7 we analyze translation times at right and left nodes of the tree. In Section 8 we obtain the lower bound of $n^5(\log d)^2$ for the maximum computing time of the bisection method.

In Section 9 we discuss previous work on upper dominance bounds for the maximum computing time of the bisection method in Johnson (1998), Krandick (1995) and Eigenwillig et al. (2006). In Section 10 we introduce an improvement of the bisection method and prove that its maximum computing is dominated by $n^5(\log d)^2$.

2. The roots of $A_{a,n}$

We begin with some theorems about the real and complex roots of $A_{a,n}$.

Theorem 1. *$A_{a,n}$ has exactly three positive real roots, namely one in each of the intervals $(0, 1/a)$, $(1/a, 1)$ and $(1, \infty)$.*

Proof. $A_{a.n}(0) = -2 < 0$, $A_{a,n}(1/a) = 1/a^n > 0$, $A_{a,n}(1) = 1 - 2(a-1)^2 \le 1 - 2 < 0$ and $A_{a,n}(\infty) > 0$ so there is at least one root in each of the named intervals. But $A_{a,n}$ has only three coefficient sign variations so by the Descartes rule each interval contains only one root. □

Let these three roots be called r_1, r_2 and r_3, $r_1 < r_2 < r_3$. Mignotte (1981) gave a sketchy and slightly incorrect proof that $r_1, r_2 \in (1/a - h, 1/a + h)$ where $h = a^{-n/2-1}$. In fact this is not true for $a = 2$ and $n \le 7$. Krandick (1995) gave a correct proof of the following theorem,

Theorem 2. *Let $h = a^{-n/2-1}$. Then if $a \ge 3$ or if $a = 2$ and $n \ge 7$ then $r_1 \in (1/a - h, 1/a)$ and $r_2 \in (1/a, 1/a + h)$.*

In the following we will not use the case $a = 2$.

Theorem 3. *Let C be the circle of radius 1 centered at the origin. If $a \ge 2$ then r_1 and r_2 are the only roots of $A_{a,n}$ inside of C.*

Proof. We use Rouche's theorem, which can be found, for example, in Marden (1949). It states that if C is a simple closed Jordan curve and $P(z)$ and $Q(x)$ are analytic inside of C and continuous on C and if $|P(z)| < |Q(z)|$ on C then $P(z) + Q(z)$ has the same number of zeros inside of C as $Q(z)$. We apply it with C the circle of radius 1 centered at the origin, $P(z) = z^n$ and $Q(z) = -2(az-1)^2$. Clearly $|P(z)| = 1$ everywhere on C and $|Q(z)| = 2|az-1|^2$ so it suffices to prove that $|az-1|^2 \ge 1$ on C. At $z = x + yi$,

$$|az-1|^2 = |(ax-1) + (ay)i|^2 = (ax-1)^2 + (ay)^2 = a^2x^2 - 2ax + 1 + a^2y^2.$$

On C, $y^2 = 1 - x^2$. Substituting we obtain

$$a^2x^2 - 2ax + 1 + a^2y^2 = -2ax + 1 + a^2.$$

Then, since $-1 \le x \le 1$ on C and $a \ge 2$,

$$-2ax + 1 + a^2 \ge -2a + 1 + a^2 = (a-1)^2 \ge 1. \qquad \square$$

Theorem 4. *$A_{a,n}$ is irreducible and therefore has no rational roots.*

Proof. The irreducibility of $A_{a,n}$ is a consequence of Eisenstein's irreducibility criterion using the prime number 2. □

3. Notation and structure

We will let T be the translation transformation $\mathrm{T}(P(x)) = P(x+1)$. Then T^k is the translation $\mathrm{T}^k(P(x)) = P(x+k)$. We will also let H be the homothetic transformation $\mathrm{H}(P(x)) = 2^n P(x/2)$, where n is the degree of P. Then $\mathrm{H}^k(P(x)) = 2^{kn}(P(x/2^k))$. We let R be the reversion transformation $\mathrm{R}(P(x)) = x^n P(1/x)$, where n is again the degree of P. We will let $\mathrm{var}(P)$ be the number of coefficient sign variations of P.

When applied to $A_{a,n}$ the bisection method computes k such that 2^k is an upper bound for the positive roots of $A_{a,n}$. The method will then proceed to find h, $0 \le h < k$, such that $(2^h, \infty)$ is an isolating interval for r_3 and then continue on to find that all other positive roots are in $(0, 1)$. At this stage the method will have an associated transformed polynomial that is $A_{a,n}$. We will ignore the time used up to this point and prove that just the time to isolate the two roots in $(0, 1)$ dominates $n^5(\ln a)^2$. Actually this is not true when a is a power of 2, say $a = 2^k$, since in this case the bisection method quickly finds the isolating interval $(0, 1/2^k)$ in time dominated by $n^3k^2 \sim n^3(\ln a)^2$. We believe that the time dominates $n^5(\ln a)^2 \sim n^5(\ln d)^2$ for every a that is not a power of 2, but for simplicity we will only prove this for odd a.

We will use some of the notation and concepts of Rouillier and Zimmermann (2004). Specifically there is a binary tree associated with the computation in which each node has a label (k, c) where k is the level of the node in the tree and $0 \le c < 2^k$. The root node is $(0, 0)$ and the two subnodes of node (k, c) are $(k+1, 2c)$ and $(k+1, 2c+1)$. Each node has an associated interval $I_{k,c} = (c/2^k, (c+1)/2^k)$ and an associated transformed polynomial $P_{k,c}$. $P_{0,0} = P$, the input polynomial. $P_{k+1,2c} = \mathrm{H}(P_{k,c})$ and $P_{k+1,2c+1} = \mathrm{T}(\mathrm{H}(P_{k,c}))$. It then follows by induction on k, using the identity $\mathrm{H}(\mathrm{T}(P)) = \mathrm{T}^2(\mathrm{H}(P))$ that, for all k and c, $P_{k,c} = \mathrm{T}^c(\mathrm{H}^k(P))$. (See Theorem 10 below.) Notice also that $\mathrm{T}^c = \mathrm{T}_c$ (translation by c).

4. The binary tree for $A_{a,n}$

Let us now consider the binary tree when the input polynomial is a Mignotte polynomial $A_{a,n}$, a is odd, $a \ge 3$ and the initial interval is $(0, 1)$. At each level of the tree there will be just one internal node (k, c), the one such that $I_{k,c}$ contains r_1 and r_2 and therefore also $1/a$. We can therefore characterize the binary tree by a finite sequence b_k, $k \ge 1$, of binary digits 0 and 1 such that $b_k = 0$ if the internal node at level k is the left subnode of the internal node at level $k-1$, $b_k = 1$ otherwise. The sequence terminates when the midpoint of $I_{k,c}$ is between r_1 and r_2.

There is a well-known algorithm (see, e.g., Hardy and Wright, 1960) for computing the infinite binary expansion of $1/a$ when a is an odd positive integer. Namely set $c_0 = 1$; then compute $c_{i+1} = 2c_i \bmod a$ and set $b_{i+1} = 1$ if $2c_i > a$, $b_{i+1} = 0$ otherwise. For some m, $1 \le m < a$, $c_m = 1$. Then the cycle $b_1 \cdots b_m$ repeats ad infinitum. For example, the binary expansion of $1/5$ is $.00110011\cdots$. The cycle 0011 repeats endlessly.

In all following theorems it is implicitly assumed that a is odd and $a \ge 3$.

Definition. N_k is the internal node at level k, I_k is the interval of N_k and $e_k/2^k$ is the left endpoint of I_k. $b_1b_2 \ldots b_m$ is the cycle in the binary expansion $.b_1b_2b_3\ldots$ of $1/a$

Theorem 5. *$e_k = \lfloor 2^k/a \rfloor < 2^k/a$.*

Proof. We prove that $e_k = \lfloor 2^k/a \rfloor$ by induction on k. If $k = 0$ then $0 = e_k = \lfloor 2^0/a \rfloor$. Assume that $e_k = \lfloor 2^k/a \rfloor$ and let $2^k = e_k a + c_k$. If $c_k < a/2$ then $2^{k+1} = 2e_k a + 2c_k$ with $2c_k < a$ so $e_{k+1} = \lfloor 2^{k+1}/a \rfloor = 2e_k$. Otherwise $2^{k+1} = 2e_k a + 2c_k$ with $2a > 2c_k > a$ so $2^{k+1} = (2e_k+1)a + (2c_k - a)$ with $0 < 2c_k - a < a$ and therefore $e_{k+1} = 2e_k + 1$. The inequality follows because 2^k is even and a is odd. □

Theorem 6. *$e_{k+1} = 2e_k$ if $b_{k+1} = 0$ and $e_{k+1} = 2e_k + 1$ if $b_{k+1} = 1$.*

Proof. $b_1b_2\ldots b_k = \lfloor 2^k/a \rfloor = e_k$ for all $k \ge 0$ by Theorem 5, so $e_{k+1} = 2e_k$ if $b_{k+1} = 0$. and $b_{k+1} = 1$ if $e_{k+1} = 2e_k + 1$. □

Theorem 7. *N_{k+1} is the left subnode or the right subnode of N_k according as b_{k+1} is 0 or 1.*

Proof. This follows from Theorem 7 since e_{k+1} is $2e_k$ for the left subnode, $2e_k+1$ for the right subnode. □

Theorem 8. $1/a - e_k/2^k < 1/2^k$.

Proof. $e_k/2^k = .b_1b_2\dots b_k$. Subtracting $e_k/2^k$ from the binary expansion of $1/a$ we obtain $1/a - e_k/2^k = .0\dots 0b_{k+1}b_{k+2}\dots < 1/2^k$. □

Theorem 9. *Let k be greatest such that $e_k/2^k < r_1$. Then $k+2 > \frac{n}{2}\log_2(a)$.*

Proof. By hypothesis $e_k/2^k < r_1$ but $e_{k+1}/2^{k+1} > r_1$. By Theorem 2, $r_1 > 1/a - h$. Therefore $e_{k+1}/2^{k+1} > 1/a - h$ and from this it follows that $1/a - e_{k+1}/2^{k+1} = \sum_{i=k+2}^{\infty} b_i/2^i < h$. Let j be least such that $j \ge k+2$ and $b_j = 1$. Then $1/2^j < h$. There can be at most $\lfloor \log_2(a) \rfloor - 1$ consecutive zeroes in the binary expansion of $1/a$ and $b_{k+1} = 1$, so $j \le k+2+\lfloor \log_2(a) \rfloor$. Therefore $1/2^{k+2+\lfloor \log_2(a) \rfloor} < h = a^{-n/2-1}$. Inverting, $2^{k+2+\lfloor \log_2(a) \rfloor} > a^{n/2+1}$. Applying logarithms, $k+2+\log_2(a) > (n/2+1)\log_2(a)$. Subtracting $\log_2(a)$ from each side, $k+2 > \frac{n}{2}\log_2(a)$. □

5. The transformed polynomials

Let P_k be the transformed polynomial associated with the internal node N_k. Thus $P_0 = P = A_{a,n}$.

Theorem 10. *If A is any polynomial then $H(T(A)) = T(H(A))$.*

Proof. Let $A(x) = \sum_{i=0}^{n} a_i x^i$, $B(x) = \mathrm{T}(A(x)) = \sum_{i=0}^{n} b_i x^i$ and $C(x) = \mathrm{H}(B(x)) = \sum_{i=0}^{n} c_i x^i$. Then $b_i = \sum_{j=i}^{n} \binom{j}{i} a_j$ and $c_i = 2^{n-i} b_i = \sum_{j=i}^{n} \binom{j}{i} 2^{n-i} a_j$. Let $D(x) = \sum_{i=0}^{n} d_i x^i = \mathrm{H}(A(x))$ and $E(x) = \sum_{i=0}^{n} e_i x^i = \mathrm{T}^2(D(x))$. Then $d_i = 2^{n-i} a_i$ and $e_i = \sum_{j=i}^{n} \binom{j}{i} 2^{j-i} d_j = \sum_{j=i}^{n} \binom{j}{i} 2^{j-i}(2^{n-j} a_i) = \sum_{j=i}^{n} \binom{j}{i} 2^{n-i} a_i = c_i$. Therefore $E = C$. □

Theorem 11. *If $A(x)$ and $B(x)$ are arbitrary polynomials then $T(A+B) = T(A) + T(B)$.*

Proof. Let n be the maximum of the degrees of A and B, $A(x) = \sum_{i=0}^{n} a_i x^i$, $B(x) = \sum_{i=0}^{n} b_i x^i$, $\bar{A}(x) = \sum_{i=0}^{n} \bar{a}_i x^i = \mathrm{T}(A(x))$ and $\bar{B}(x) = \sum_{i=0}^{n} \bar{b}_i x^i = \mathrm{T}(B(x))$. Then $\bar{a}_i = \sum_{j=i}^{n} \binom{j}{i} a_j$ and $\bar{b}_i = \sum_{j=i}^{n} \binom{j}{i} b_j$ so $\bar{a}_i + \bar{b}_i = \binom{j}{i}(a_j + b_j) = \binom{j}{i} a_j + \binom{j}{i} b_j$ is the coefficient of x^i in $\mathrm{T}(A(x)) + \mathrm{T}(B(x))$ and also in $\mathrm{T}(A+B)(x)$. □

Theorem 12. *If A and B are arbitrary nonzero polynomials then $H(AB) = H(A)H(B)$.*

Proof. Let $A(x) = \sum_{i=0}^{m} a_i x^i$, $B(x) = \sum_{j=0}^{n} b_j x^j$, $C(x) = A(x)B(x) = \sum_{k=0}^{m+n} c_k x^k$, $\deg(A) = m$ and $\deg(B) = n$. Then $\mathrm{H}(A(x)) = \sum_{i=0}^{m} 2^{m-i} a_i x^i$ and $\mathrm{H}(B(x)) = \sum_{j=0}^{n} 2^{n-j} b_j$. Multiplying,

$$\mathrm{H}(A(x))\mathrm{H}(B(x)) = \sum_{k=0}^{m+n} \sum_{i+j=k} 2^{m+n-k} c_k x^k = \mathrm{H}(C(x)). \qquad \square$$

Theorem 13. *If $0 \le k \le K$ then $P_k = T^{e_k}(H^k(P))$.*

Proof. By induction on k. If $k = 0$ then $e_k = 0$ so $P_k = \mathrm{T}^0(\mathrm{H}^0(P_k))$. Assume $0 \le k < K$ and $P_k = \mathrm{T}^{e_k}(\mathrm{H}^k(P))$. By Theorem 7, if $b_k = 0$ then $e_{k+1} = 2e_k$ and $P_{k+1} = \mathrm{H}(P_k) = \mathrm{H}(\mathrm{T}^{e_k}(\mathrm{H}^k(P_k))) = \mathrm{T}^{2e_k}(\mathrm{H}^{k+1}(P_k))$ by Theorem 10 applied e_k times. If $b_k = 1$ then, by Theorem 7, $P_{k+1} = \mathrm{T}^{e_k+1}(\mathrm{H}^k(P_k)) = \mathrm{T}(\mathrm{H}(\mathrm{T}^{e_k}(\mathrm{H}^k(P_k)))) = \mathrm{T}(\mathrm{T}^{2e_k}(\mathrm{H}^{k+1}(P_k))) = \mathrm{T}^{2e_k+1}(\mathrm{H}^{k+1}(P_k)) = \mathrm{T}^{e_{k+1}}(\mathrm{H}^{k+1}(P_k))$ by Theorem 7. □

Theorem 14. $T^{e_k}(H^k(P(x))) = T^{e_k}(x^n) - 2^{k(n-2)+1}T^{e_k}(H^k(ax-1)^2)$.

Proof.

$$\begin{aligned}\mathrm{H}^k(P(x)) &= \mathrm{H}^k(x^n - 2(ax-1)^2) = x^n - 2^{k(n-2)+1}(a^2x^2 - 2^{k+1}ax + 2^{2k})\\ &= x^n - 2^{k(n-2)+1}(ax-2^k)^2\\ &= x^n - 2^{k(n-2)+1}(\mathrm{H}^k(ax-1))^2.\end{aligned}$$

Now apply Theorem 11 e_k times with $A(x) = x^n$ and $B(x) = -2^{k(n-2)+1}(\mathrm{H}^k(ax-1))^2$. □

Theorem 15. *Let* $0 \le k \le K$ *and* $P_k(x) = \sum_{i=0}^{n} p_{k,i}x^i$. *Then*

$$\begin{aligned}p_{k,0} &= -2^{k(n-2)+1}(ae_k - 2^k)^2 + e_k^n,\\ p_{k,1} &= -2^{k(n-2)+1}2a(ae_k - 2^k) + ne_k^{n-1},\\ p_{k,2} &= -2^{k(n-2)+1}a^2 + \binom{n}{2}e_k^{n-2},\end{aligned}$$

and, for $3 \le i \le n$,

$$p_{k,i} = \binom{n}{i}e_k^{n-i}.$$

Proof. By Theorem 14,

$$\begin{aligned}P_k(x) = \mathrm{T}^{e_k}(\mathrm{H}^k(P)) &= \mathrm{T}^{e_k}(x^n) - 2^{k(n-2)+1}T^{e_k}(\mathrm{H}^k(ax-1))^2\\ &= (x+e_k)^n - 2^{k(n-2)+1}(a(x+e_k) - 2^k)^2\\ &= (x+e_k)^n - 2^{k(n-2)+1}(a^2x^2 + 2a(ae_k - 2^k)x + (ae_k - 2^k)^2).\end{aligned}$$

Now apply the binomial theorem to $(x+e_k)^n$ and add coefficients. □

Theorem 16. *Let* $0 \le k \le K$ *and* $H(P_k(x)) = \bar{P}_k(x) = \sum_{i=0}^{n} \bar{p}_{k,i}x^i$. *Then*

$$\begin{aligned}\bar{p}_{k,0} &= -2^{(k+1)(n-2)+1}(2ae_k - 2^{k+1})^2 + (2e_k)^n,\\ \bar{p}_{k,1} &= -2^{(k+1)(n-2)+1}2a(2ae_k - 2^{k+1}) + n(2e_k)^{n-1},\\ \bar{p}_{k,2} &= -2^{(k+1)(n-2)+1}a^2 + \binom{n}{2}(2e_k)^{n-2},\end{aligned}$$

and, for $3 \le i \le n$,

$$\bar{p}_{k,i} = \binom{n}{i}(2e_k)^{n-i}.$$

Proof. By Theorem 13 and Theorem 10, $\bar{P}_k(x) = \mathrm{H}(P_k(x)) = \mathrm{H}(\mathrm{T}^{e_k}(\mathrm{H}^k(P(x)))) = \mathrm{T}^{2e_k}(\mathrm{H}^{k+1}(P(x)))$. Now proceed as in the proof of Theorem 15. □

6. Translation time when $b_k = 1$

We will assume that the subadditivity theorem is used. For added clarity let us use U for the transformation TR, which maps $(0,1)$ onto $(0,\infty)$. This theorem asserts that for an arbitrary polynomial A, if $A_1 = \mathrm{H}(A)$ and $A_2 = \mathrm{T}(A_1)$ then $\mathrm{var}(\mathrm{U}(A_1)) + \mathrm{var}(\mathrm{U}(A_2)) \le \mathrm{var}(\mathrm{U}(A))$. If $\mathrm{var}(\mathrm{U}(A))$ is the number of variations of A in $(0,1)$ then $\mathrm{var}(\mathrm{U}(A_1))$ is the number of variations in $(0,\frac{1}{2})$ and $\mathrm{var}(\mathrm{U}(A_2))$ is the number of variations in $(\frac{1}{2}, 1)$. If subadditivity is not used then both $\mathrm{UH}(P_k)$ and $\mathrm{UHT}(P_k)$ must always be computed. But if $\mathrm{var}(\mathrm{UH}(P_k))$ is computed first and is equal to $\mathrm{var}(P_k)$ then $\mathrm{UHT}(P_k)$ does not need to be computed, saving two translations. So we assume that $\mathrm{UH}(P_k)$ is always computed first.

We will first prove that whenever $\mathrm{var}(\mathrm{UH}(P_k)) = 0$, which is when $b_k = 1$, then the time to compute the translation of $\mathrm{RH}(P_k)$ dominates kn^3. This would suffice to prove that the time to isolate the two roots of $A_{a,n}$ in $(0, 1)$ dominates $n^5(\ln a)^2$ if we knew that there is some positive lower bound for the density of 1's in the binary expansion of $1/a$, a odd. In fact there is no such lower bound since the density is only $1/k$ when $a = 2^k - 1$. If we eliminate such a's then the existence of a lower bound is in doubt even if we require a to be a prime. For primes less than one million other than those of the form $2^k - 1$ there are just five with densities less than $1/3$, shown below.

431	.302
1801	.280
2351	.319
122 921	.286
178 481	.217

The translation array of a polynomial is defined in Collins (2016), Definition 61.

Theorem 17. *Let A be the translation array for the translation by 1 of $R(\bar{P}_k)$. If $k < \frac{1}{2}(n(\lg a - 1)) - \frac{3}{2}$ then, in column 0 of A, $A_{i,0} \le -2^{(k+1)(n-2)}$ for $2 \le i \le n$.*

Proof. The leading three coefficients of $R(\bar{P}_k)$ are the three last coefficients of $\bar{P}_k$, which are given in Theorem 16. $A_{i,0}$, $i \ge 2$, is the sum of the three low order coefficients of $\bar{P}_k$ plus some of the coefficients in the binomial expansion of $(x + 2e_k)^n$. By Theorem 16, for $i \ge 3$ the sum of the i lowest-order coefficients of $\bar{P}_k$ is equal to $-E_1 + E_2$, where

$$E_1 = 2^{(k+1)(n-2)+1}((2ae_k - 2^{k+1})^2 + 2a(2ae_k - 2^{k+1}) + a^2),$$
$$E_2 = (2e_k)^n + n(2e_k)^{n-1} + \sum_{i=2}^{n} \binom{n}{i} (2e_k)^{n-i}.$$

$(2ae_k - 2^{k+1})^2 + 2a(2ae_k - 2^{K+1}) + a^2 = ((2ae_k - 2^{k+1}) + a)^2 \ge 1$ since $((2ae_k - 2^{k+1}) + a)$ is an odd integer. Therefore $E_1 \ge 2^{(k+1)(n-2)+1}$ and so the theorem is proved if $e_k = 0$. Otherwise $e_k \ge 1$. Then

$$\lg(E_1) \ge (k+1)(n-2) + 1.$$

$E_2 < (2e_k + 1)^n$ by the binomial theorem and $(2e_k + 1)^n < (4e_k)^n < 4^n(2^k/a)^n$. Therefore

$$\lg(E_2) < kn + 2n - n \lg a.$$

$((k+1)(n-2)+1) - (kn + 2n - n \lg a) = -2k - n + n \lg a - 1$, which is at least 1 since by hypothesis $2k < n \lg a - n - 3$. Therefore $E_2 \le \frac{1}{2}E_1$, which implies that $-E_1 + E_2 \le -\frac{1}{2}E_1 \le -2^{(k+1)(n-2)}$. □

Theorem 18. *If $0 \le k \le K$ then $\bar{p}_{k,0} + \bar{p}_{k,1} > 2^{(k+1)(n-2)+3}$.*

Proof. By Theorem 16, $\bar{p}_{k,0} + \bar{p}_{k,1} = -2^{(k+1)(n-2)+3}(ae_k - 2^k)(ae_k - 2^k + a) + 4e_k^n + 2ne_k^{n-1}$. By Theorem 6, $ae_k - 2^k = a(e_k - 2^k/a) < 0$ and $ae_k - 2^k + a = a(e_k + 1) - 2^k = a((e_k + 1) - 2^k/a) > 0$. Therefore $(ae_k - 2^k)(ae_k - 2^k + a) < 0$ and, since a is odd, $(ae_k - 2^k)(ae_k - 2^k + a) \le -1$. Therefore $-2^{(k+1)(n-2)+3}(ae_k - 2^k)(ae_k - 2^k + a) \ge 2^{(k+1)(n-2)+3}$. Since $4e_k^n + 2ne_k^{n-1} \ge 0$ this completes the proof. □

Theorem 19. *If $b_k = 1$ and $1 \le k < \frac{n}{2}(\lg a - 1)$ then $2\bar{p}_{k,0} + \bar{p}_{k,1} < -2^{(k+1)(n-2)+2}$.*

Proof. Applying Theorem 16, $2\bar{p}_{k,0} + \bar{p}_{k,1} = -E_1 + E_2$, where

$$\begin{aligned} E_1 &= 2^{(k+1)(n-2)+1}(2ae_k - 2^{k+1})(2ae_k - 2^{k+1} + 2a) \\ &= 2^{(k+1)(n-2)+3}(ae_k - 2^k)(ae_k - 2^k + a) \end{aligned}$$

and $E_2 = (2e_k)^n + n(2e_k)^{n-1}$. By Theorem 6, since $ae_k - 2^k = a(e_k - 2^k/a)$, $-a < ae_k - 2^k < 0$. Therefore $ae_k - 2^k + a > 0$. Since a is odd, $ae_k - 2^k \le -1$ and $ae_k - 2^k + a \ge 1$. Therefore $E_1 \ge 2^{(k+1)(n-2)+3}$.

$E_2 < (2e_k + 1)^n < (4e_k)^n < 4^n(2^k/a)^n$.

$\lg(E_1) \ge (k+1)(n-2)+3$ and $\lg(E_2) < kn + 2n - n\lg a$. Therefore $E_2 \le \frac{1}{2}E_1$ provided that $kn + 2n - n\lg a \le (k+1)(n-2) + 2$, equivalently $2k \le n(\lg a - 1)$, which is hypothesized. Therefore $E_1 \le \frac{1}{2}E_2$, which implies $-E_1 + E_2 \le -\frac{1}{2}E_1 \le 2^{(k+1)(n-2)+2}$. □

Theorem 20. *Let $C = 2^{(k+1)(n-2)}$. If $b_k = 1$ and $1 \le k < \frac{n}{2}\lg a - \frac{1}{2}$ then $\bar{p}_{k,0} < -\frac{1}{2}C$.*

Proof. By Theorem 16, $\bar{p}_{k,0} < -8C + (2e_k)^n$. $(2e_k)^n < 2^n(2^k/a)^n = 2^{(k+1)n}/a^n$. Therefore $\lg((2e_k)^n) < (k+1)n - n\lg a$ whereas $\lg(8C) = kn + n - 2k + 1$. Therefore $\lg(8C) - \lg((2e_k)^n = -2k + 1 + n\lg a$, which by hypothesis is greater than $(-2k - 1 + n\lg a) + 1$. Therefore $(2e_k)^n < \frac{1}{2}C$ and so $-C + (2e_k)^n < -\frac{1}{2}C$. □

Theorem 21. *Assume that $b_k = 1$ and $1 \le k \le \frac{n}{2}\lg a - \frac{n}{2} - \frac{3}{2}$. Let $C = 2^{(k+1)(n-2)}$. Let A be the translation array for $R(\bar{P}_k)$. Then $|A_{1,j}| \ge \frac{1}{2}C$ for $i \ge 0$ and $j \ge 0$. Only $A_{1,0}$ is positive.*

Proof. By Theorem 20, every element of row 0 is less than $-\frac{1}{2}C$. By Theorem 18, $A_{1,0} > 8C$. By Theorem 19, $A_{1.1} = 2\bar{p}_{k,0} + \bar{p}_{k,1} < -4C$. Then since, by Theorem 20, $\bar{p}_{k,0} < -\frac{1}{2}C$, $A_{1,j} = A_{1,1} + (j-1)\bar{p}_{k,0} < -4C$ for $j \ge 2$. By Theorem 7, $A_{i,0} \le -C$ for $i \ge 2$. Then by induction on i and j, $A_{i,j} \le -C$ for $i \ge 2$ and $j \ge 1$, being the sum of two numbers each of which is $\le -C$. □

Theorem 22. *For $b_k = 1$ and $1 \le k \le \frac{n}{2}\lg a - \frac{n}{2} - \frac{3}{2}$, the time to translate $R(\bar{P}_k)$ dominates kn^3.*

Proof. By Theorem 21, the computation of $A_{i,j}$ for $i \ge 0$ and $j \ge 1$ requires the addition of two integers, each in absolute value greater than or equal to $2^{(k+1)(n-2)-1}$ and thus takes time dominating $(k+1)(n-2) - 1$, which dominates kn. The number of such additions is $\binom{n+1}{2}$, which dominates n^2, so the total translation time dominates kn^3. □

7. Translation time when $b_k = 0$

Now suppose that $b_k = 0$.

Theorem 23. *Let $0 \le k \le K$ and $H(P_k(x)) = \bar{P}_k(x) = \sum_{i=0}^{n} \bar{p}_{k,i}x^i$. Let $C = 2^{(k+1)(n-2)+1}a^{2.}$. Let $f_k = e_k - 2^k/a$. Then*

$$\begin{aligned} \bar{p}_{k,0} &= -C \cdot 4f_k^2 + (2e_k)^n, \\ \bar{p}_{k,1} &= -C \cdot 4f_k + n(2e_k)^{n-1}, \\ \bar{p}_{k,2} &= -C + \binom{n}{2}(2e_k)^{n-2}, \end{aligned}$$

and, for $3 \le i \le n$,

$$\bar{p}_{k,i} = \binom{n}{i}(2e_k)^{n-i}.$$

Proof. By Theorem 16,

$$\begin{aligned}\bar{p}_{k,0} &= -C(2ae_k - 2^{k+1})^2/a^2 + (2e_k)^n \\ &= -C(2e_k - 2^{k+1}/a)^2 + (2e_k)^n \\ &= -C \cdot 4f_k^2 + (2e_k)^n.\end{aligned}$$

Derivation of the formulas $\bar{p}_{k,1} = -C \cdot 4f_k + n(2e_k)^{n-1}$ and $\bar{p}_{k,2} = -C + \binom{n}{2}(2e_k)^{n-2}$ from Theorem 16 is similar and the formula for $\bar{p}_{k,i}$, $i \geq 3$, is just a restatement of Theorem 16. $\square$

Let A be the translation array for $\mathrm{R}(\bar{P}_k)$. In the next several theorems we derive a sufficient condition on k such that every element of row m is negative.

Theorem 24. *If $A(x) = \sum_{i=0}^{n} a_i x^i$ is any polynomial of degree n and A is the translation array for $A(x)$ then, for all i and j,*

$$A_{i,j} = \binom{i+j}{j} a_n + \binom{i+j-1}{j} a_{n-1} + \cdots + \binom{j}{j} a_{n-j}.$$

Proof. This a restatement of Theorem 81 of Collins and Krandick (2012). $\square$

Theorem 25. *Let $C = 2^{(k+1)(n-2)+1}$ and $f_k = e_k - 2^k/a$. Then $A_{m.j} = -E_1 + E_2$, where*

$$E_1 = \left\{4\binom{m+j}{j} f_k^2 + 4\binom{m+j-1}{j} f_k + \binom{m+j-2}{j}\right\} Ca^2$$

and

$$E_2 = \sum_{i=0}^{j} \binom{m+j-i}{j}\binom{n}{i}(2e_k)^{n-i}.$$

Proof. This follows from Theorem 24 applied to $\mathrm{R}(\bar{P}_k)$ and the use of Theorem 23. $\square$

Theorem 26. *Let $|f_k| \leq \frac{1}{15}$ and $m = \lfloor n/2 \rfloor \geq 3$. Then, for $0 \leq j \leq m$,*

$$E_1 = \{4\binom{m+j}{j} f_k^2 + 4\binom{m+j-1}{j} f_k + \binom{m+j-2}{j}\}Ca^2 \geq C.$$

Proof. $\binom{m+j-2}{j}/\binom{m+j-1}{j} = \frac{m-1}{m+j-1} \geq \frac{2}{5}$. Also $4\binom{m+j}{j} f_k^2 \geq 0$. Therefore $E_1 \geq (4f_k + \frac{2}{5})\binom{m+j-1}{j}Ca^2 \geq (-\frac{4}{15} + \frac{2}{5})\binom{m+j-1}{j}Ca^2 = \frac{2}{15}\binom{m+j-1}{j}Ca^2 \geq C$ since $a \geq 3$. $\square$

Theorem 27. *Assume $e_k > 0$. Then $E_2 < 2^{kn+3n+1}/a^n$.*

Proof.

$$\sum_{i=0}^{j} \binom{m+j-1}{j}\binom{n}{i}(2e_k)^{n-i} \leq \left\{\sum_{i=0}^{j} \binom{m+j-i}{j}\right\}\left\{\sum_{i=0}^{j} \binom{n}{i}(2e_k)^{n-i}\right\}$$

$$\sum_{i=0}^{j} \binom{m+j-i}{j} = \binom{m+j+1}{j} < 2^{m+j+1} < 2^{n+1}$$

$$\sum_{i=0}^{j}\binom{n}{i}(2e_k)^{n-i} < \sum_{i=0}^{n}\binom{n}{i}(2e_k)^{n-i} = (2e_k+1)^n$$
$$< (4e_k)^n = 2^{2n}e_k^n < 2^{2n}(2^k/a)^n = 2^{kn+2n}/a^n.$$

Combining the above inequalities yields $E_2 < 2^{kn+3n+1}/a^n$. $\square$

Theorem 28. *Assume that $e_k > 0$, $|f_k| \le \frac{1}{15}$, $n \ge 6$ and $k \le \frac{n}{2}(\lg a - 2) - \frac{3}{2}$. Then $A_{m,j} = -E_1 + E_2 < 0$ for $0 \le j \le m$.*

Proof. By Theorem 26, $E_1 \ge C = 2^{(k+1)(n-2)}$. Therefore $\lg(E_1) \ge (k+1)(n-2)$. By Theorem 27, $E_2 < 2^{kn+3n+1}/a^n$. Therefore $\lg(E_2) \le kn + 3n + 1 - n\lg a$. So $\lg(E_1) - \lg(E_2) \ge (k+1)(n-2) - kn - 3n - 1 + n\lg a = -2k - 2n - 3 + n\lg a$. By hypothesis, $-2k + n\lg a - 2n - 3 \ge 0$. So $\lg(E_1) > \lg(E_2)$. Therefore $E_1 > E_2$ and $-E_1 + E_2 < 0$. $\square$

Theorem 29. *Assume $e_k > 0$, $|f_k| \le \frac{1}{15}$, $n \ge 6$ and $k \le \frac{n}{2}(\lg a - 2) - \frac{3}{2}$. Then The time required to translate $R(\bar{P}_k)$ dominates kn^3.*

Proof. By Theorem 17, in the translation array for $\mathrm{R}(\bar{P}_k)$, $A_{i,0} \le -C$ for $m \le i \le n$. By Theorem 28, $A_{m,j} < 0$ for $j \ge 1$. Since $A_{m+1,0} \le -C$ it follows that $A_{m+1,j} \le -C$ for $j > 0$ by induction on j. Then by induction on i, it follows that $A_{i,j} < -C$ for $m+1 \le i \le n$ and $0 \le j \le n-i$. Therefore $A_{i,j}$ is computed as the sum $A_{i,j-1} + A_{i-1,j}$ with both summands less than $-C$ for $i \ge m+1$ and $1 \le j \le n-i$. The number of such additions is $\binom{n-m}{2}$, which dominates n^2. Since the time for each addition dominates $(k+1)(n-2)$, which dominates kn, the total time dominates kn^3. $\square$

8. Total translation time

Now we consider the time for all translations.

Theorem 30. *Let $n \ge 6$, $e_k > 0$ and $k + 4 \le \frac{n}{2}(\lg a - 2) - \frac{3}{2}$. Then for some j, $k \le j \le k+4$, the time for the translation of $R(\bar{P}_j)$ dominates kn^3.*

Proof. If $b_j = 1$ for some j in $[k, k+4]$ then the time for translation of $\mathrm{R}(\bar{P}_j)$ dominates jn^3 and hence kn^3 by Theorem 22. Otherwise $b_j = 0$ for all j in $[k, k+4]$. Then $e_{j+1} = 2e_j$ for j in $[k, k+4]$. Therefore $f_{j+1} = 2f_j$ for j in $[k, k+4]$. Since $|f_{k+4}| < 1$, $|f_k| < \frac{1}{16}$ and therefore, by Theorem 29, the time to translate $\mathrm{R}(\bar{P}_k)$ dominates kn^3. $\square$

Theorem 31. *The total translation time dominates $n^5(\lg a)^2$ for $n \ge 8$ and $a \ge 65$.*

Proof. Let $k_1 = \lceil \lg a \rceil$. Then $e_k > 0$ for $k > k_1$. Let $k_2 = \lfloor \frac{n}{2}\lg a - n - \frac{11}{2} \rfloor$. Partition the interval $[k_1, k_2]$ into $\lfloor (k_2 - k_1 + 1)/5 \rfloor$ intervals $[k_1, k_1+4]$, $[k_1+5,\ k_1+9]$, etc. Then by Theorem 30 the translation time for the j-th such interval dominates $(k_1+5j)n^3 \succeq jn^3$. $k_2 - k_1 + 1 \ge \frac{n}{2}(\lg a - 2) - \frac{13}{2} - \lg a - 1 = \frac{n}{2}(\lg a - 2) - \frac{13}{2} - (\lg a - 2) + 1 = (\frac{n}{2} - 1)(\lg a - 2) - \frac{11}{2}$. Using $n \ge 8$, $\frac{n}{2} - 1 \ge \frac{3}{8}n$ so $k_2 - k_1 + 1 \ge \frac{3}{8}n(\lg a - 2) - \frac{11}{2}$. Then, since $\lg a \ge 6$, $\lg a - 2 \ge \frac{2}{3}\lg a$ and therefore $k_2 - k_1 + 1 \ge \frac{1}{4}n\lg a - \frac{11}{2}$. Since $n \ge 8$, $k_2 - k_1 + 1 \ge 2n\lg a - \frac{11}{2}$ and $(k_2 - k + 1)/5 \ge \frac{2}{5}n\lg a - \frac{11}{10} \ge \frac{96}{5} - \frac{11}{10} = \frac{181}{10} \ge 18$. Therefore the number of intervals dominates $n\lg a$. and the translation time for these intervals dominates $\sum_{j=1}^{n\lfloor \lg a \rfloor} jn^3 \succeq n^5(\lg a)^2$. $\square$

Theorem 32. *The total translation time dominates $n^5(\lg a)^2$ for $n \ge 8$ and $33 \le a \le 63$.*

Proof. The proof of this theorem is similar to that of Theorem 31, but here we use Theorem 22 instead of Theorem 30. $k_2 = \lfloor \frac{n}{2}(\lg a - 1) - \frac{3}{2} \rfloor$ and $k_1 = \lceil \lg a \rceil$ as before. Because $\lg a < 6$, $b_k = 0$ for at most five consecutive values of k, partition the interval $[k_1, k_2]$ into $\lfloor (k_2 - k_1 + 1)/6 \rfloor$ intervals $[k_1, k_1 + 5]$, $[k_1 + 6, k_1 + 11]$, etc. Then by Theorem 22 the time for the translations in the j-th interval dominates jn^3. $k_2 - k_1 + 1 \geq (\frac{n}{2}(\lg a - 1) - \frac{3}{2} - 1) - 6 = \frac{n}{2}(\lg a - 1) - \frac{17}{2}$, so $\lfloor (k_2 - k_1 + 1)/6 \rfloor \geq \lfloor \frac{n}{12}(\lg a - 1) - \frac{17}{12} \rfloor \geq \lfloor \frac{n}{3} - \frac{17}{12} \rfloor \geq \lfloor \frac{8}{3} - \frac{17}{12} \rfloor = 1$. Therefore the number of intervals dominates $\frac{n}{2}(\lg a - 1) \succeq n \lg a$ and, by Theorem 22, the time for the translations dominates $\sum_{j=1}^{n\lfloor \lg a \rfloor} jn^3 \succeq n^5 (\lg a)^2$. □

Theorem 33. *The total translation time dominates $n^5(\lg a)^2$ for $n \geq 8$ and $17 \leq a \leq 31$.*

Proof. The proof is like that of Theorem 32 but now $4 < \lg a < 5$ and the interval $[k_1, k_2]$ is partitioned into intervals of five elements. The number of intervals is at least $\lfloor (k_2 - k_1 + 1)/5 \rfloor \geq (\frac{n}{2} \cdot 4 - \frac{3}{2} - 5)/5 \geq \frac{2}{5}n - 2 \geq 1$. $(\frac{n}{2}(\lg a - 1) - \frac{3}{2} - 1) - \lceil \lg a \rceil)/5 \geq (\frac{n}{2} \cdot \frac{3}{4} \lg a - \frac{5}{2})/5 = (\frac{3}{8} n \lg a - \frac{5}{2})/5 \geq \frac{3}{40} n \lg a - \frac{1}{2} \geq \frac{3}{40} \cdot 32 - \frac{1}{2} > 1$ so the number of intervals dominates $n \lg a$. □

Theorem 34. *The total translation time dominates $n^5(\lg a)^2$ for $n \geq 8$ and $9 \leq a \leq 15$.*

Proof. Like that of Theorem 33, now with $3 < \lg a < 4$ and intervals of four elements. The number of intervals is at least $\lfloor ((\frac{n}{2}(\lg a - 1) - \frac{3}{2}) - 4 + 1)/4 \rfloor = \lfloor (\frac{n}{2}(\lg a - 1) - \frac{9}{2})/4 \rfloor \geq \lfloor \frac{1}{3} n \lg a - \frac{9}{8}) \rfloor \geq \lfloor n - \frac{9}{8} \rfloor > 6$. So the number of intervals dominates $n \lg a$. □

Theorem 35. *The total translation time dominates $n^5(\lg a)^2$ for $n \geq 8$ and $a = 7$.*

Proof. Assume $n = 7$. Then $\lg a \geq 11/4$ so $(\lg a - 1)/\lg a \geq \frac{7}{11}$. Therefore $k_2 \geq \lfloor \frac{7}{22} n \lg a - \frac{3}{2} \rfloor \geq \frac{7}{22} n \lg a - \frac{5}{2}$. $k_2 = 3$ so Theorem 22 is applicable provided that $\lfloor (k_2 - k_1 + 1)/3 \rfloor \geq \lfloor (\frac{7}{22} n \lg a - \frac{9}{2})/3 \rfloor > 0$. This condition is equivalent to $\frac{7}{66} n \lg a - \frac{3}{2} \geq 1$, which is not true if $n = 8$ but is true if $n \geq 9$. So the total translation time dominates $n^5(\lg a)^2$ for $n \geq 9$ and $a = 7$ by Theorem 22. But trivially the translation time dominates $n^5(\lg a)^2$ for $n = 8$ and $a = 7$, completing the proof. □

Theorem 36. *The total translation time dominates $n^5(\lg a)^2$ for $n \geq 8$ and $a = 5$.*

Proof. The proof is like that of Theorem 35 and uses $\lg 5 \geq \frac{9}{4}$. $(\lg a - 1)/\lg a \geq \frac{5}{9}$ so $k_2 \geq \lfloor \frac{5}{18} n \lg a - \frac{3}{2} \rfloor \geq \frac{5}{18} n \lg a - \frac{5}{2}$. $k_2 = 3$ so Theorem 23 is applicable provided that $\lfloor (\frac{5}{18} n \lg a - \frac{9}{2})/3 \rfloor > 0$, equivalently that $\frac{5}{54} n \lg a - \frac{3}{2} \geq 1$. This condition is satisfied if $n \geq 12$. Translation time trivially dominates $n^5(\lg a)^2$ on the finite set $\{8, 9, 10, 11\}$. □

Theorem 37. *The total translation time dominates $n^5(\lg a)^2$ for $n \geq 8$ and $a = 3$.*

Proof. One more application of the proof pattern of the two preceding theorems. $\lg 3 \geq \frac{11}{7}$ so $(\lg a - 1)/\lg a \geq \frac{4}{11}$. $k_2 = 2$ so the use of Theorem 22 requires that $\lfloor (\frac{2}{11} n \lg a - \frac{7}{2})/2 \rfloor \geq 0$, equivalently that $\frac{1}{11} n \lg a - \frac{7}{4} \geq 1$. This holds if $n \geq 20$. So the translation time dominates $n^5(\lg a)^2$ for $a = 3$ and $n \geq 20$. It does so trivially on the finite set $8 \leq n \leq 19$. □

Theorem 38. *The computing time of the bisection method with $A_{a,n}$ as input, a odd, $a \geq 3$ and $n \geq 8$, dominates $n^5(\lg a)^2$*

Proof. Theorems 31–37 partition the set $\{n \geq 8 \wedge \mathrm{odd}(a) \wedge a \geq 3\}$ into seven subsets on each of which the computing time dominates $n^5(\lg a)^2$. □

Theorem 39. *The maximum computing time of the bisection method for polynomials of degree n and max norm d dominates* $n^5(\log d)^2$.

Proof. The max norm d of $A_{a,n}$ for $a \geq 3$ is $2a^2$. Therefore $\log d \sim \log a$. So this theorem is a consequence of Theorem 38. □

9. Upper bound on the computing time

In 1991 in his Ph.d. dissertation at Ohio State University, Johnson stated in a theorem, p. 116, that the computing time of the bisection method is dominated by $n^5(\log d)^2$ with d being the sum norm of A, but his proof ignored the increase in coefficient size when a root bound is applied. Krandick (1995) remedied this, proving in Satz 50, that the computing time is dominated by $n^5(\log d)^2$ provided that all positive roots of A are less than 1. But to ensure this condition on the roots it is necessary in general to apply this theorem to $A(bx)$ where b is a root bound. Since b can be as large as d, the max norm of $A(bx)$ can be as large as d^n and then the computing time to isolate all positive roots of $A(x)$ is dominated only by $n^5(\log d^n) \sim n^7(\log d)^2$. In 1998 Johnson's 1991 proof was published (Johnson, 1998).

Krandick (1995) had already proved the bound $n^5(\log nd)^2$ where d is the max norm of $A(bx)$ and b is a power of 2 upper bound for the positive roots of A. Krandick's proof is careful and correct in all details but Johnson does not cite it.

Johnson stated his result with d as the sum norm $|A|_1$. Krandick stated his result with d as the Euclidean norm, $|A|_2$. The Euclidean norm is needed only in applying Davenport's theorem. I can find no place in Johnson's proof where the sum norm is needed. It is routinely assumed, usually implicitly, in codominance analyses that the degree n is a single-precision integer, equivalently that $\ln n$ is bounded. Without this assumption nearly all operations on polynomials would have computing times dependent on $\log n$, equivalently the bit length of n. Both Johnson's proof and Krandick's use the assumption without mention. But, in spite of this, Krandick did not simplify $(\log nd)^2$ to $(\log d)^2$ in his result. Assuming that $\log n$ is bounded, the norm that is used in stating the bound is immaterial because then $|A| \sim |A|_1 \sim |A|_2$.

The proofs of Johnson and Krandick proceed by bounding the time for a specific level of the bisection tree. Eigenwillig et al. (2006) asserted a dominance bound of $n^5(\log d)^2$ for the polynomial $A(bx)$, where b is a bound for the positive roots of $A(x)$. Their proof proceeds by bounding the number of nodes in the bisection tree and then bounding the time required at any node of the tree. Their proof applies to the transformed polynomial resulting after applying a root bound. If their proof is correct this is a very significant accomplishment but their proof is sketchy. In particular there are two assertions in the proof requiring elaboration. One such assertion is that a node "has bit cost $O(n^2(nL + nh))$". This seems to ignore the fact that a translation has a cost that includes a term in n^3. The missing elaboration here is that n^3 is dominated by $n^2(nL + nh)$. The L in their proof is the same as $\lg d$ where d is the max norm of the polynomial. Another place where elaboration is needed is where it is asserted that the transformation from $A(x)$ to $A(bx)$ does not increase the size of the recursion tree, or at least does not increase it from $O(n(L + \log n))$ to $O(n(L' + \log n))$ where L' is the maximum bit size of the transformed polynomial $A(bx)$. This seems to suggest that it does increase it some, but there is no discussion of how much it can be increased.

10. Improvement of the method

The transformation $\mathrm{H}(A(x)) = 2^n A(x/2)$ should act as the inverse of the transformation $A(2x)$ but it doesn't. $\mathrm{H}(A(2x)) = 2^n A(x)$ and this is the reason that the maximum computing time of the bisection method as it has hitherto been presented is $n^7(\ln d)^2$. This problem can be fixed by defining $\mathrm{H}(A(x))$ to be $A(x/2)$ when it is known that $A(x)$ is equal to $B(2x)$ for some $B(x)$. This presents the question of how this shall be determined. The question could be answered computationally. It is true just in case that, for every i, the coefficient a_i has at least i trailing zero bits, so the computation can be carried out in time dominated by only n^2. Alternatively it can be answered by keeping track of the level in the binary tree of the computation to which the polynomial belongs. The modification of the bisection method that does so will be called the improved bisection method. That this is so follows from the following theorem.

Theorem 40. *For every integral polynomial $A(x)$ there is an integral polynomial $B(x)$ such that $T(A(2x)) = B(2x)$.*

Proof. The coefficient of x^i in $A(2x)$ is divisible by 2^i. The coefficient of x^i in $\mathrm{T}(A(2x))$ is an integer linear combination of the coefficients of x^j in $A(2x)$ such that $j \geq i$. Therefore the coefficient of x^i in $\mathrm{T}(A(2x))$ is divisible by 2^i. $\square$

The modification of the bisection method that utilizes this strategy will be called the *improved* bisection method.

Now consider the binary tree of the improved bisection method when the input is an arbitrary squarefree univariate polynomial $A(x)$ with max norm d. As in Section 3, each node has a label (h, c) where h is the level of the node and $0 \leq c \leq 2^h - 1$. We assume that an upper bound $b = 2^e$, e a nonnegative integer, has been computed for the positive roots of A. We may also assume that $2^e \leq 4d$ since if $A(x) = \sum_{i=0}^{n} a_i x^i$ then $|a_i/a_n|^{1/(n-i)} \leq d$ for all $i < n$. Therefore e is dominated by $\ln d$.

We will obtain a dominance upper bound of $n^5(\ln d)$ for the computing time of the improved bisection method by analyzing separately the computing times for all nodes at levels less than or equal to e and for all nodes greater than e, where 2^e is a root bound.

Theorem 41. *Let d be the max norm of A and let 2^e be the root bound for A. For the improved method the computation time for all nodes at levels less than or equal to e is dominated by $n^4(\ln d)^2$.*

Proof. For $h \leq e$, every polynomial at level h is a translation $\mathrm{T}^m(A(2^{e-h}x))$ with $m < 2^h$. The max norm of $A(2^{e-h}x)$ is at most $2^e d$ so the max norm of $\mathrm{T}^m(A(2^{e-h}x))$ is at most $(2^e d)(2^{h(n+1)})$ and the time for its translation by 1 is dominated by $n^3 + n^2 \ln(2^{e+h(n+1)}d) \preceq n^3 + n^2(e + hn + \ln d) \preceq hn^3 + n^2 \ln d \preceq n^3 \ln d$. Since the number of translations by 1 at each level is dominated by n, the total time for all levels less than e is dominated by $en(n^3 \ln d) \preceq n^4(\ln d)^2$. $\square$

Theorem 42. *Let d be the max norm of A and let 2^e be the root bound for A. For the improved method the computation time for all nodes at levels greater than e is dominated by $n^5(\ln d)^2$.*

Proof. For $h > e$, every polynomial at level h is a translation $\mathrm{T}^m(2^{n(h-e)}A(x/2^{h-e}))$ with $m < 2^h$ and therefore has a max norm that is at most $(2^{n(h-e)})(2^{h(n+1)})d \leq 2^{2hn+1}d$. Therefore the time required to translate it by 1 is dominated by $n^3 + n^2(2hn+1)d \preceq hn^3 d$. By application of Satz 48 of Krandick (1995) to the polynomial $A(2^e x)$, if there are k nodes at level h, then $hk \preceq n \ln(2^e d) \preceq ne + n \ln d \preceq n \ln d$, so the time for all translations of level h polynomials is dominated by $hkn^3 \preceq n^4 \ln d$. Also by Satz 48 the height of the tree is dominated by $n \ln d$, so the time for all translations is dominated by $(n \ln d)(n^4 \ln d) \sim n^5(\ln d)^2$. $\square$

Theorem 43. *The maximum computing time of the improved bisection method for a polynomial A of degree n and max norm d is codominant with $n^5(\ln d)^2$,*

Proof. The proof in the first 8 sections of this paper that the maximum computing time of the bisection method dominates $n^5(\ln d)^2$ clearly holds also for the improved method. Theorems 41 and 42 together prove that the maximum computing time of the improved method is dominated by $n^5(\ln d)^2$. $\square$

References

Collins, George E., 2016. Continued fraction real root isolation using the Hong root bound. J. Symb. Comput. 72, 21–54.

Collins, George E., Akritas, Alkiviadis G., 1976. Polynomial real root isolation using Descartes' rule of signs. In: Jenks, R.D. (Ed.), Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation. ACM Press, pp. 272–275.

Collins, George E., Krandick, Werner, 2012. On the computing time of the continued fractions method. J. Symb. Comput. 47, 1372–1412.

Eigenwillig, Arno, Sharma, Vikram, Yap, Chee K., 2006. Almost tight recursion tree bounds for the Descartes method. In: Dumas, J.-G. (Ed.), International Symposium on Symbolic and Algebraic Computation. ACM Press, pp. 71–78.

Hardy, G.H., Wright, E.M., 1960. An Introduction to the Theory of Numbers, fourth edition. Oxford University Press.

Johnson, J.R., 1998. Algorithms for polynomial real root isolation. In: Caviness, B.F., Johnson, J.R. (Eds.), Quantifier Elimination and Cylindrical Algebraic Decomposition. Springer-Verlag, pp. 269–299.

Krandick, Werner, 1995. Isolierung reeller Nullstellen von Polynomen. In: Herzberger, J. (Ed.), Wissenschaftliches Rechnen. Akademie Verlag, Berlin, pp. 105–154.

Marden, Morris, 1949. The Geometry of the Zeros of a Polynomial in a Complex Variable. Mathematical Surveys, vol. III. American Mathematical Society.

Mignotte, Maurice, 1981. Some inequalities about univariate polynomials. In: Proceedings of the ACM Symposium on Symbolic and Algebraic Computation, pp. 195–199.

Rouillier, Fabrice, Zimmermann, Paul, 2004. Efficient isolation of polynomial's real roots. J. Comput. Appl. Math. 162, 33–50.