Journal of Computational and Applied Mathematics 384 (2021) 113169

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

How to count the number of zeros that a polynomial has on the unit circle?

R.S. Vieira[1]

Universidade Federal de São Carlos (UFSCar), Departamento de Matemática, Rod. Washington Luís, km. 235 SP-310, CEP. 13565-905, São Carlos, São Paulo, Brazil

ARTICLE INFO

Article history:
Received 18 May 2019
Received in revised form 11 June 2020

Keywords:
Self-inversive polynomials
Self-reciprocal polynomials
Salem polynomials
Sturm theorem
Möbius transformations
Cayley transformations

ABSTRACT

The classical problem of counting the number of real zeros of a real polynomial was solved a long time ago by Sturm. The analogous problem of counting the number of zeros that a polynomial has on the unit circle is, however, still an open problem. In this paper, we show that the second problem can be reduced to the first one through the use of a suitable pair of Möbius transformations – often called Cayley transformations – that have the property of mapping the unit circle onto the real line and vice versa. Although the method applies to arbitrary complex polynomials, we discuss in detail several classes of polynomials with symmetric zeros as, for instance, the cases of self-conjugate, self-adjoint, self-inversive, self-reciprocal and skew-reciprocal polynomials. Finally, an application of this method to Salem polynomials and to polynomials with small Mahler measure is also discussed.

1. Methods for counting the number of real zeros of real polynomials

The first exact method for counting the number of zeros that a real polynomial has on the real line (or in a given interval of the real line) was presented by Sturm in 1829 (see [1], p. 323). In its simplest form, Sturm algorithm works as follows: given a real polynomial $p(z)$ of degree n, let $a < b$ be two real numbers which are not a multiple zero of $p(z)$. Then, construct the so-called *Sturm sequence*,[2] $S(z) = \{S_0(z), S_1(z), S_2(z), \dots, S_m(z)\}$, whose elements are defined as follows:

$$S_0(z) = p(z), \qquad S_1(z) = p'(z), \qquad \text{and} \qquad S_k(z) = -\text{rem}\left[S_{k-2}(z), S_{k-1}(z)\right], \qquad 2 \leqslant k \leqslant m, \tag{1.1}$$

where $p'(z)$ is the derivative of $p(z)$, rem $[A, B]$ denotes the remainder of the polynomial division of A by B and m is the integer determined from the condition that $S_m(z)$ has degree zero. Now, let var $[S(\zeta)]$ denote the number of sign variations in the sequence $S(z)$ for $z = \zeta$. Then, Sturm showed that the number N of distinct zeros of $p(z)$ in the half-open interval $\mathcal{I} = (a, b]$ is, just, $N = \text{var}[S(a)] - \text{var}[S(b)]$. This is the content of the so-called *Sturm theorem*, whose proof can be found in many places — see, for example, [2]. It works because as we vary z from a to b on the real line the sequence $S(z)$ suffers a sign variation when, and only when, z passes through a zero of $p(z)$; thus, the number of sign variations of $S(z)$ from a to b exactly counts the number of distinct real zeros of $p(z)$ in this interval. Considering the interval $\mathcal{I}$ as the whole real line, the number of real zeros of $p(z)$ is obtained (Sturm algorithm in this case can be further simplified,

E-mail address: ricardovieira@ufscar.br.

1 ORCID: 0000-0002-8343-7106.

2 This is the *classical Sturm sequence*. For the definition of more general Sturm sequences, see [2].

https://doi.org/10.1016/j.cam.2020.113169
0377-0427/

as it is enough to keep only the leading terms of the polynomials $S_k(z)$, which asymptotically dominates the behaviour of these polynomials).

Notice that Sturm sequence is constructed in very similar fashion as the sequence of remainders obtained in computation of the greatest common divisor (GCD) of the polynomials $p(z)$ and $p'(z)$: the only difference is that we should keep the *opposite* of the polynomial remainders in each step. Alternatively, we could compute the ordinary sequence $R = \{r_0(z), r_1(z), r_2(z), \ldots, r_m(z)\}$ of the remainders obtained in the computation of the GCD of $p(z)$ and $p'(z)$ (where $r_0(z) = p(z)$, $r_1(z) = p'(z)$ and $r_k(z) = \text{rem}\,[r_{k-2}(z), r_{k-1}(z)]$, $2 \leqslant k \leqslant m$), from which the Sturm sequence can be obtained by negating the signs of each two consecutive remainders $r_k(z)$ as follows:

$$S = \{r_0(z), r_1(z), -r_2(z), -r_3(z), r_4(z), r_5(z), -r_6(z), -r_7(z), r_8(z), r_8(z), \ldots\}\,. \tag{1.2}$$

This can be easily shown by comparing the construction of the two sequences and noticing that the quotients $t_k(z)$ appearing in Sturm's sequence are related with the respective quotients $q_k(z)$, obtained in the GCD of $p(z)$ and $p'(z)$, through the formula $t_k(z) = (-1)^{k+1} q_k(z)$. This relationship shows us that the complexity of Sturm algorithm is the same as the complexity of the GCD of $p(z)$ and $p'(z)$.

We remark that Sturm's method requires $p(z)$ a real polynomial with no multiple zeros at the endpoints a and b, although $p(z)$ may have multiple zeros in the open interval (a, b). Notice also that the counting excludes that eventual zero at $z = a$ but includes the zero at $z = b$; it is, however, an easy matter to verify if $p(z)$ has or not a zero at $z = a$, so that we can also count the number of zeros of $p(z)$ in any closed interval $[a, b]$ of the real line. Besides, keep in mind that the Sturm algorithm counts only the number of *distinct* real zeros of $p(z)$. This issue, however, can be overcome by additional analysis.[3]

It is worth to mention that Sturm derived this theorem during his researches on qualitative aspects of differential equations, which gave rise to the so-called *Sturm–Liouville theory*. In fact, in an interval of weeks, Sturm published similar theorems regarding the distribution of zeros of orthogonal functions, which are solutions of Sturm–Liouville differential equation [1]. Sturm was influenced by the works of Fourier and, as a matter of a fact, his method can be thought of as a refinement of Fourier's previous result [4] that establishes an upper bound for the number of real zeros of $p(z)$ in a given half-open interval $(a, b]$ of the real line through the number of sign variations in the *Fourier sequence* $F(z) = \left\{p(z), p'(z), \ldots, p^{(n)}(z)\right\}$, for z running from a to b over the real line. Thus, we can say that Sturm's method makes Fourier's exact.

Since the publication of Sturm's fundamental papers, other methods for counting or isolating the real zeros of a given real polynomial were formulated. In 1834, Vincent published a paper [5] (republished two years later, with few additions, in [6]), in which a method based on successive replacements in terms of continued fractions was proposed. His method was based on a previous work of Budan [7], who established a theorem equivalent to that of Fourier commented above, although in a different form. Unfortunately, Vincent's work was almost forgotten thenceforward and, in fact, it was only rescued from oblivion in 1976 by Collins and Akritas, who formulated a powerful bisection method based on Vincent's theorem for isolating the zeros of a given real polynomial [8]. Two years later, Akritas [9] gave a fundamental contribution to this method by replacing the uniform substitutions that take place in Vincent's algorithm by non-uniform ones based on previously calculated bounds for the zeros of the testing polynomial (with that modification, Akritas was able to reduce the complexity of Vincent's method from exponential to polynomial type). Further improvements of these methods, among with new symbolic and numeric techniques, gave rise to some of the fastest algorithms known to date for counting or isolating the zeros of real polynomials on the real line [10–15] and also on regions of the complex plane [16–23].

2. The Cayley transformations and polynomials

The methods described above determine the exact number of zeros of a real polynomial on the real line $\mathbb{R}$. The correspondent problem of determining the exact number of zeros of a given polynomial on the unit circle is still unsolved. In fact, this is an old question whose first works remount to the end of XIX century, for instance, the pioneer works Eneström, Kakeya, Schur, Kempner, Cohn, among others — see [24] and references therein. In the recent years, a great interest in this problem has emerged, usually in connection with the theory of the so-called *self-inversive polynomials*. These are complex polynomials whose zeros are all symmetric with respect to the unit circle (real self-inversive polynomials includes the *self-reciprocal* and the *skew-reciprocal* polynomials). These classes of polynomials are very important in both pure and applied mathematics, as they appear in several problems related to the theory of numbers, algebraic curves, knots theory, stability theory, dynamic systems, error-correcting codes, cryptography and even in classical, quantum and statistical mechanics — see [24] and references therein. An important question regarding self-inversive and self-reciprocal polynomials is the number of zeros that these polynomials have in the unit circle $\mathbb{S} = \{z \in \mathbb{C} : |z| = 1\}$. There are a countless number of papers devoted to the question of finding conditions for all, some, or no zero of a self-inversive polynomial to lie on $\mathbb{S}$, see [24].

[3] Indeed, Sturm himself had shown in a subsequent paper (see [1] p. 345) that the number of non-real zeros of $p(z)$ in the interval $(a, b]$ can also be determined from his method by other arguments. Moreover, from a generalization of Sturm algorithm due to Thomas [3], the multiplicity of the zeros are counted directly.

In this paper, we present a method that reduces the problem of counting the number of zeros that an arbitrary complex polynomial has on the unit circle to the problem of counting the number of zeros of a real polynomial on the real line. Because the second problem is completely addressed by Sturm (or any other real root-counting) algorithm, our approach also solves the first problem completely. The method is based on the use of the following pair of Möbius transformations:

$$\mu(z) = (z-i)/(z+i), \qquad \text{and} \qquad \omega(z) = -i\,(z+1)/(z-1), \tag{2.1}$$

which are often called *Cayley transformations*. Together with the relations $\mu(\infty) = 1$, $\mu(-i) = \infty$ and $\omega(1) = \infty$, $\omega(\infty) = -i$, these two transformations become the inverse of each other in the extended complex plane $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$. It can be easily verified that $\mu(z)$ maps the real line onto the complex unit circle, while $\omega(z)$ maps the unit circle onto the real line.[4] Besides, $\mu(z)$ sends any point in the upper-half (lower-half) plane to the interior (exterior) of $\mathbb{S}$, so that $\omega(z)$ sends any point in the inside (outside) of $\mathbb{S}$ to the upper-half (lower-half) plane.

Given a complex polynomial $p(z)$ of degree n, we define the *transformed polynomials* $q_\mu(z)$ and $q_\omega(z)$ by the formulas:

$$q_\mu(z) = (z+i)^n\, p(\mu(z)), \qquad \text{and} \qquad q_\omega(z) = \left(\tfrac{i}{2}\right)^n (z-1)^n\, p(\omega(z)). \tag{2.2}$$

The factor $\left(\frac{i}{2}\right)^n$ in front of the second formula in (2.2) is to make the two mappings the inverse each of the other. The following theorems discuss some properties of these transformed polynomials and their zeros.

Theorem 1. *Let $p(z)$ be a complex polynomial of degree n. If $p(z)$ has a zero of multiplicity m at the point $z = 1$, then $q_\mu(z)$ defined as above will be a polynomial of degree $n - m$. Similarly, if $p(z)$ has a zero of multiplicity m at the point $z = -i$, then $q_\omega(z)$ defined as above will be a polynomial of degree $n - m$.*

Proof. Suppose that $p(z)$ has a zero at $z = 1$ of multiplicity m, where $0 \leqslant m \leqslant n$. Write, $p(z) = (z-1)^m\, r(z)$, where $r(z)$ is a polynomial of degree $n - m$ with no zeros at $z = 1$. From (2.2) we get that $q_\mu(z) = (-2i)^m\, s(z)$, where $s(z) = (z+i)^{n-m}\, r(\mu(z))$. Now, expanding $s(z)$ in powers of z we can verify that its leading coefficient equals $r(1)$; because $r(1) \neq 0$ we conclude that $s(z)$ is a polynomial of degree $n - m$ and so it is $q_\mu(z)$. By the same argument, if $p(z)$ has a zero of multiplicity m at the point $z = -i$, then, from (2.2) we get that $q_\omega(z)$ will be is a polynomial of degree $n - m$. □

Thus, the condition for the transformed polynomial $q_\mu(z)$ (respectively, $q_\omega(z)$) to have the same degree as the original polynomial $p(z)$ is that $p(z)$ has no zero at $z = 1$ (respectively, at $z = -i$).

Theorem 2. *Let $\zeta_1, \ldots, \zeta_n$ be the zeros of a complex polynomial $p(z)$ of degree n. If $p(1) \neq 0$, then the zeros of the transformed polynomials $q_\mu(z)$ will be, respectively, $\xi_1 = \omega(\zeta_1), \ldots, \xi_n = \omega(\zeta_n)$. Similarly, if $p(-i) \neq 0$, then the zeros of the transformed polynomial $q_\omega(z)$ will be, respectively, $\eta_1 = \mu(\zeta_1), \ldots, \eta_n = \mu(\zeta_n)$.*

Proof. Inverting the first equation in (2.2), we get that $p(\zeta_k) = \left(\frac{i}{2}\right)^n (\zeta_k - 1)^n\, q_\mu(\omega(\zeta_k)) = 0$, $1 \leqslant k \leqslant n$, but $\zeta_k \neq 1$ which means that $\xi_k = \omega(\zeta_k)$ is a zero of $q_\mu(z)$. Similarly, inverting the second equation in (2.2) we get that $p(\zeta_k) = (\zeta_k + i)^n\, q_\omega(\mu(\zeta_k)) = 0$, $1 \leqslant k \leqslant n$, and the condition $\zeta_k \neq 1$ implies that $\eta_k = \mu(\zeta_k)$ is a zero of $q_\omega(z)$. □

Theorem 2 shows us that whenever a polynomial is transformed through a Cayley transformation, its zeros are accordingly transformed through the inverse transformation. Besides, from the relations $\mu(-i) = \infty$ and $\omega(1) = \infty$, we see that if $p(z)$ has a zero at the point $z = 1$ (respectively, $z = -i$), then the transformed polynomial $q_\mu(z)$ (respectively, $q_\omega(z)$) will have a zero at infinity, which confirms again that the transformed polynomial cannot have the same degree as $p(z)$ in these cases.

The previous results imply the following theorem, which is a keystone in what follows:

Theorem 3. *Let $p(z)$ be a complex polynomial of degree n that has m zeros on $\mathbb{S}$, counted with multiplicity, and such that $p(1) \neq 0$. Then the transformed polynomial $q_\mu(z)$ will have exactly m zeros on $\mathbb{R}$, also counted with multiplicity. Similarly, if $p(z)$ is a complex polynomial of degree n that has m zeros on $\mathbb{R}$, counted with multiplicity, and such that $p(-i) \neq 0$, then the transformed polynomial $q_\omega(z)$ will have m zeros on $\mathbb{S}$, also counted with multiplicity.*

Proof. These statements follow directly from theorems proved above and from the fact that the Cayley transformations $\mu(z)$ and $\omega(z)$ map $\mathbb{R}$ on $\mathbb{S}$ and vice versa, respectively. □

The following complements Theorem 3:

Theorem 4. *Let $p(z)$ be a complex polynomial of degree n that has exactly $2m$ zeros symmetric to $\mathbb{S}$ and such that $p(1) \neq 0$. Then, the polynomial $q_\mu(z)$ will have exactly $2m$ zeros symmetric to $\mathbb{R}$ (i.e., complex conjugate zeros). Conversely, if $p(z)$ is a complex polynomial of degree n that has precisely $2m$ zeros symmetric to $\mathbb{R}$ and such that $p(-i) \neq 0$, then the polynomial $q_\omega(z)$ will have precisely $2m$ zeros symmetric to $\mathbb{S}$.*

4 We remark that the transformations (2.1) are not the only pair of Möbius transformations that maps $\mathbb{S}$ onto $\mathbb{R}$ and vice versa: they are, however, the most adequate ones for our purposes.

Proof. Let ζ and $1/\zeta^\star$ be any pair of zeros of $p(z)$ that are symmetric to $\mathbb{S}$.[5] The corresponding zeros of $q_\mu(z)$ will be $\xi = \omega(\zeta)$ and $\chi = \omega(1/\zeta^\star)$. However, from (2.1) we can easily show that $\omega(1/\zeta^\star) = \omega^\star(\zeta)$, so that $\chi = \xi^\star$. Similarly, if ζ and $\zeta^\star$ are any complex conjugate pair of zeros of $p(z)$, then it follows that the corresponding zeros of $q_\omega(z)$ are $\eta = \mu(\zeta)$ and $\sigma = \mu(\zeta^\star)$. But from (2.1) we can show that $\mu(\zeta^\star) = 1/\mu^\star(\zeta)$, so that $\sigma = 1/\eta^\star$. □

3. General complex polynomials

It is clear from Theorem 3 how we can count the number of zeros that a polynomial $p(z)$ of degree n has on the unit circle: all we need to do is to compute the transformed polynomial $q_\mu(z) = (z+i)^n p(\mu(z))$ and then use some *real-root-counting* (RRC) method to count the number of zeros of $q_\mu(z)$ on the real line.[6] Some care should be taken, however, depending on whether method we use to this end. For example, as mentioned in Section 1, Sturm and Akritas methods do not take into account the multiplicity of the zeros of the testing polynomials; if we want to account the multiplicities, then a suitable RRC method should be employed to this end — for example, Thomas algorithm [3]. Besides, we shall see that the action of the Cayley transformation over a polynomial $p(z)$ usually results in a non-real polynomial even when $p(z)$ is real,[7] whereas most of the RRC methods need a real polynomial to work with — including Sturm or Akritas methods. Thus, whenever $q_\mu(z)$ is not a real polynomial, an auxiliary real polynomial $Q(z)$, which has the same number of zeros on $\mathbb{R}$ than $q_\mu(z)$, should be found.

Algorithm 1A: General complex polynomials

input : A complex polynomial $p(z)$ of degree n.
output: The number of distinct zeros of $p(z)$ on the unit circle.

$n := \text{degree}(p(z))$;
$q(z) := (z+i)^n\, p\left(\frac{z-i}{z+i}\right)$;
if $q(z) \neq q^\star(z^\star)$ **then** $q(z) \leftarrow q(z)q^\star(z^\star)$ **end**;
$N := \text{RRC}\,[q(z), -\infty, \infty]$;
if $p(1) = 0$ **then** $N \leftarrow N+1$ **end**;
return N.

Algorithm 1B: General complex polynomials (alternative)

input : A complex polynomial $p(z)$ of degree n.
output: The number of distinct zeros of $p(z)$ on the unit circle.

$n := \text{degree}(p(z))$;
$q(z) := (z+i)^n\, p\left(\frac{z-i}{z+i}\right)$;
if $q(z) \neq q^\star(z^\star)$ **then**
  $r(z) := \frac{1}{2}\left[q(z) + q^\star(z^\star)\right]$;
  $s(z) := \frac{1}{2i}\left[q(z) - q^\star(z^\star)\right]$;
  $q(z) \leftarrow \text{GCD}[r(z), s(z)]$
end
$N := \text{RRC}\,[q(z), -\infty, \infty]$;
if $p(1) = 0$ **then** $N \leftarrow N+1$ **end**;
return N.

In what follows, we shall present algorithms[8] that allow one to compute the number of zeros that a polynomial $p(z)$ of degree n has on $\mathbb{S}$. First we shall present general algorithms that work with an arbitrary complex-polynomial; then, specific algorithms that take into account the symmetry of the zeros of the testing polynomials regarding $\mathbb{S}$ or $\mathbb{R}$ will be

---

5 The star means complex conjugation so that, if $p(z) = \sum_{k=0}^{n} p_k z^k$, then $p(z^\star) = \sum_{k=0}^{n} p_k (z^\star)^k$, $p^\star(z) = \sum_{k=0}^{n} p_k^\star (z^\star)^k$ and $p^\star(z^\star) = \sum_{k=0}^{n} p_k^\star z^k$.

6 We mention that the idea of using a Möbius transformation to verify if a given polynomial has some zero on the unit circle is not new, although this topic seems to not have been explored in detail before. Indeed, as far as we know, such possibility was discussed only in some old references due to Kempner [25,26] and, more recently, in an expository note due to Conrad [27] (who credited F. Rodriguez-Villegas for this idea). We remark, however, that Kempner considered a only real polynomial $p(z)$, while the transformed polynomial $q(z)$ was defined through the formula, $q(z) = \left(z^2+1\right) p\left(\frac{z-i}{z+i}\right) p\left(\frac{z+i}{z-i}\right)$; this essentially corresponds to the case discussed by us in Algorithm 3. Conrad, on the other hand, made no mention to Sturm algorithm or any other RCC method.

7 We shall see in Theorem 8 that the transformed polynomial $q_\mu(z) = (z+i)^n p(\mu(z))$ will be a real polynomial only if the original polynomial $p(z)$ is self-adjoint.

8 For the sake of simplicity, hereafter we shall consider that the RRC method employed in the algorithms has the same properties as those of Sturm's method. The symbol $\text{RRC}\,[q(z), \alpha, \beta]$ will denote an RRC procedure that gives the exact number of *distinct* zeros that a real polynomial $q(z)$ has on the interval $(\alpha, \beta]$ of the real line.

presented. The asymptotic complexities of these algorithms are all the same, as the RRC procedures used in the algorithms are the most time-consuming part of them (for the complexity of Sturm and Akritas algorithms, see [2]). Nonetheless, when comparing polynomials of the same degree we shall see that the specific algorithms are usually faster because they deliver a polynomial of smaller degree to the RRC procedure.

Let us begin with the case where the testing polynomial $p(z)$ is an arbitrary complex polynomial of degree n. From (2.2), it follows that the transformed polynomial $q_\mu(z)$ will usually have non-real coefficients. Thus, provided that the RRC procedure works only with a real polynomial, we need to find an auxiliary polynomial $Q(z)$, with real coefficients, that has the same number of zeros on $\mathbb{R}$ as does $q_\mu(z)$. We can overcome this issue in two ways: The first way consists of multiplying the transformed polynomial $q_\mu(z)$ by its complex conjugate, $q_\mu^\star(z^\star)$, so that a polynomial of degree $2n$ is obtained in place, namely, $Q(z) = q_\mu(z)q_\mu^\star(z^\star)$. It is clear that the zeros of $q_\mu^\star(z^\star)$ are the complex conjugate of the zeros of $q_\mu(z)$, from which it follows that the real polynomial $Q(z)$ has the same number of real zeros than $q_\mu(z)$, counted without multiplicity, as required. Now we can use the RRC procedure to count the number of real zeros of $Q(z)$, which, according to Theorem 3, will correspond to the number of zeros that the original polynomial $p(z)$ has on $\mathbb{S}$, provided $p(1) \neq 0$ (if $p(1) = 0$ then all we need to do is to add 1 to the final result). This is described in Algorithm 1A. The second way consists of writing the transformed polynomial in the form $q_\mu(z) = r(z) + is(z)$, where $r(z) = \frac{1}{2}\left[q_\mu(z) + q_\mu^\star(z^\star)\right]$ and $s(z) = \frac{1}{2i}\left[q_\mu(z) - q_\mu^\star(z^\star)\right]$, so that $r(z)$ and $s(z)$ are both real polynomials. Then we can compute the GCD of $r(z)$ and $s(z)$ and define $Q(z) = \text{GCD}\,[r(z), s(z)]$. It follows that the polynomial $Q(z)$ has degree at most n and, in particular, it has the same number of zeros on $\mathbb{R}$ as does the polynomial $q_\mu(z)$. This is the content of the following:

Theorem 5. *The zeros of the polynomial $Q(z) = \text{GCD}\,[r(z), s(z)]$ are precisely the zeros of $q_\mu(z)$ whose complex conjugate is also a zero of $q_\mu(z)$. Thus, the degree of $Q(z)$ equals the number of zeros of $q_\mu(z)$ whose complex conjugate is also a zero of it, counted with multiplicity.*

Proof. We can decompose the complex polynomial $q_\mu(z)$ in a product of two polynomials, say, $q_\mu(z) = t(z)u(z)$, where $t(z)$ consists of a real polynomial that gathers all the zeros of $q_\mu(z)$ which appear in complex conjugate pairs (real zeros included), while $u(z)$ is a non-real polynomial that gathers all the remaining zeros of $q_\mu(z)$. Thus, it follows from the definition of the polynomials $r(z)$ and $s(z)$ given above that the polynomial $t(z)$ divides both $r(z)$ and $s(z)$, while $u(z)$ cannot divide both of them. Therefore, as the zeros of $Q(z) = \text{GCD}\,[r(z), s(z)]$ correspond to the common zeros of $r(z)$ and $s(z)$, the first result follows. Finally, the degree of $Q(z)$ follows from the Fundamental Theorem of Algebra. □

Algorithm 2: GENERAL COMPLEX POLYNOMIALS: ZEROS IN AN ARC OF THE UNIT CIRCLE

input : A complex polynomial $p(z)$ of degree n and two real numbers α and β such that $0 \leqslant \alpha < 2\pi$ and $0 < \beta \leqslant 2\pi$.
output: The number of distinct zeros of $p(z)$ on the arc $\mathcal{J} = (e^{i\alpha}, e^{i\beta}]$ of the unit circle.

if $\alpha = 0$ **then** $a = -\infty$ **else** $a := -i\left(\frac{e^{i\alpha}+1}{e^{i\alpha}-1}\right)$ **end**;
if $\beta = 2\pi$ **then** $b = \infty$ **else** $b := -i\left(\frac{e^{i\beta}+1}{e^{i\beta}-1}\right)$ **end**;
$n :=$ degree$(p(z))$;
$q(z) := (z+i)^n\, p\left(\frac{z-i}{z+i}\right)$;
if $q(z) \neq q^\star(z^\star)$ **then** $q(z) \leftarrow q(z)q^\star(z^\star)$ **end**;
if $\alpha > \beta$ **then**
  $N :=$ RRC$[q(z), -\infty, b]$ + RRC$[q(z), a, \infty]$;
  if $p(1) = 0$ **then** $N \leftarrow N + 1$ **end**;
  return N.
end
$N :=$ RRC $[q(z), a, b]$;
if $p(1) = 0$ **and** $b = 2\pi$ **then** $N \leftarrow N + 1$ **end**;
return N.

Notice as well that each common zero of $r(z)$ and $s(z)$ is also a zero of $q_\mu(z) = r(z) + is(z)$; the converse, however, is not true: if ξ is a zero of $q_\mu(z)$, then ξ can be either a common zero of $r(z)$ and $s(z)$ or we should have $r(\xi)/s(\xi) = -i$. The first case happens whenever ξ is a zero of $Q(z)$ – in particular when ξ is real – whence, the second case occurs whenever ξ is a zero of $q_\mu(z)$ whose complex conjugate $\xi^\star$ is not a zero of it. Therefore, to obtain a real polynomial $Q(z)$ that has the same number of zeros on $\mathbb{R}$ as does $q_\mu(z)$, we can just compute the GCD of the real polynomials $r(z)$ and $s(z)$, where $q_\mu(z) = r(z) + is(z)$. This alternative, which was already suggested in [27], is described in Algorithm 1B.

We highlight that we can also count the number of zeros of $p(z)$ in a given *arc* of the unit circle.[9] Let $\mathcal{J} = \left(e^{i\alpha}, e^{i\beta}\right]$ be the referred arc of the unit circle. In the simplest case, we assume that $0 \leqslant \alpha < \beta \leqslant 2\pi$, so that the interval $\mathcal{J}$ is mapped to the interval $\mathcal{I} = (a, b]$ of the real line, where $a = \omega(e^{i\alpha})$ and $b = \omega(e^{i\beta})$ (with the following conventions: $\lim_{\theta\to 0}\omega(e^{i\theta}) = -\infty$ and $\lim_{\theta\to 2\pi}\omega(e^{i\theta}) = \infty$). The number of zeros of $p(z)$ on the arc $\mathcal{J}$ can thereby be found by counting the number of real zeros that the polynomial $Q(z)$ (defined by one of the two possible ways as described above), has on the interval $\mathcal{I}$ of $\mathbb{R}$. In the case where $\alpha > \beta$ (which corresponds to an interval on $\mathbb{S}$ that contains the point $z = 1$), we need to split the algorithm into two parts because, in this case, the interval $\mathcal{I}$ on $\mathbb{R}$ will be composed of two

[9] This works for all the cases considered in the advance, with few modifications if necessary. For this reason we shall not comment about this possibility further (we do remark, however, that the replacement $z \leftarrow \sqrt{z}$ cannot be employed anymore to this end, as this would lead to a wrong result due to the fact that this map is not one-to-one).

disjoint intervals — namely, we have $\mathcal{I}(\alpha, \beta] = (-\infty, b] \cup (a, \infty)$. Thus, the procedure $\textsc{rrc}\,[Q(z), a, b]$ must be replaced by $\textsc{rrc}\,[Q(z), -\infty, b] + \textsc{rrc}\,[Q(z), a, \infty]$ in this case. Finally, if the point $z = 1$ belongs to the interval $\mathcal{J}$ and $p(1) = 0$, then we should add 1 to the final result. This is described in Algorithm 2 (for the sake of simplicity, we considered $Q(z) = q_{\mu}(z)q^{\star}_{\mu}(z^{\star})$ in the pseudo-code).

Moreover, it is clear that we can also locate and isolate the zeros on the unit circle of a given polynomial through these algorithms. In fact, after we map the zeros of the polynomial $p(z)$ on the unit circle to the real line through the Cayley transformations (2.1), we can find an interval $\mathcal{I} \subset \mathbb{R}$ containing all the real zeros of the transformed polynomial $q_{\mu}(z)$; then, from Sturm or Akritas procedures, we can refine this interval, for example by a bisection method, so that we obtain a list $\{\mathcal{I}_1, \dots, \mathcal{I}_n\}$ of intervals, each one containing exactly one real zero of $p(z)$ — indeed, in many symbolic computing software, is this list of isolating intervals that is returned by the implemented procedures of Sturm and Akritas, see [2,28]. This list of isolating intervals of $q_{\mu}(z)$ provides a corresponding list of arcs on the unit circle that isolate and locate the zeros of $p(z)$ on $\mathbb{S}$. These intervals can be further refined recursively so that approximated values for the zeros are returned.

Finally, notice that we can also count the number of zeros that a polynomial has in any circle or straight line of the complex plane by considering a suitable Möbius transformation $m(z) = \frac{az+b}{cz+d}$, $ad-bc \neq 0$, in place of Cayley transformation (2.1).

4. Real and self-conjugate polynomials

The algorithms presented in the previous section apply to arbitrary complex polynomials. In the most important cases, however, the coefficients of the testing polynomial enjoy certain symmetries which allow us to implement faster algorithms. Henceforward, we shall specialize in classes of polynomials whose zeros are either symmetric with respect to the real line or to the unit circle. We shall call a complex polynomial whose zeros are all symmetric to $\mathbb{R}$ as a *self-conjugate polynomial* and a complex polynomial whose zeros are all symmetric to $\mathbb{S}$ as a *self-inversive polynomial*.

Algorithm 3: SELF-CONJUGATE POLYNOMIALS

input : A self-conjugate polynomial $p(z)$ of degree n.
output: The number of distinct zeros of $p(z)$ on the unit circle.

$n :=$ degree$(p(z))$;
$q(z) := (z+i)^n \, p\left(\frac{z-i}{z+i}\right)$;
if $q(z) \neq q^{\star}(z^{\star})$ **then**
  $q(z) \leftarrow q(z)\, q^{\star}(z^{\star})$;
  $q(z) \leftarrow q(\sqrt{z})$;
  $N := 2\ \textsc{rrc}\,[q(z), 0, \infty]$;
  if $p(-1) = 0$ **then** $N \leftarrow N + 1$ **end**;
  if $p(1) = 0$ **then** $N \leftarrow N + 1$ **end**;
  return N;
end
$N := \textsc{rrc}\,[q(z), -\infty, \infty]$;
if $p(1) = 0$ **then** $N \leftarrow N + 1$ **end**;
return N.

Algorithm 4: SELF-ADJOINT POLYNOMIALS

input : A self-adjoint polynomial $p(z)$ of degree n.
output: The number of distinct zeros of $p(z)$ on the unit circle.

$n :=$ degree$(p(z))$;
$q(z) := (z+i)^n \, p\left(\frac{z-i}{z+i}\right)$;
$N := \textsc{rrc}\,[q(z), -\infty, \infty]$;
if $p(1) = 0$ **then** $N \leftarrow N + 1$ **end**;
return N.

Let us consider in this section the analysis of self-conjugate polynomials (self-inversive polynomials will be considered in the next section). If $p(z)$ is self-conjugate, then, for any zero ζ of $p(z)$, the complex conjugate number $\zeta^{\star}$ is also a zero of it. Of course, any real polynomial has this property, but there can be non-real polynomials with this property as well. The necessary and sufficient condition for a complex polynomial $p(z) = p_n z^n + \cdots + p_0$ of degree n to be self-conjugate is that $p_n \neq 0$ and that there exists a fixed complex number ϵ of modulus 1 such that, $p(z) = \epsilon p^{\star}(z^{\star})$ — see [24] for the proof. From this we can see that the coefficients of any self-conjugate polynomial $p(z)$ of degree n satisfy the properties $p_k = \epsilon p^{\star}_k$ for each ranging from 0 to n. Real polynomials are those self-conjugate polynomials with $\epsilon = 1$.

Notice that even when $p(z)$ is a real polynomial, the transformed polynomial $q_\mu(z)$ is not necessarily real. Thus, to count the number of zeros of a self-conjugate polynomial on the unit circle, we need to compute, as an intermediary step, the real polynomial $Q(z)$ by one of the two methods discussed in Section 3. However, as we shall see in the following, the polynomials $Q(z)$ have additional symmetries when $p(z)$ is self-conjugate, which allow us to improve the algorithms.

Let us first consider that $Q(z)$ is defined as $Q(z) = q_\mu(z)q^\star_\mu(z^\star)$. In this case, the following theorem shows us that if $p(z)$ is self-conjugate, then the polynomial $Q(z)$ has only even powers of z:

Theorem 6. *Let $p(z)$ be a self-conjugate polynomial of degree n such that $p(1) \neq 0$. Then, the polynomial $Q(z) = q_\mu(z)q^\star_\mu(z^\star)$ will be a real polynomial of degree n in the variable z^2.*

Proof. According to (2.2), we have that, $Q(z) = q_\mu(z)q^\star_\mu(z^\star) = (z^2+1)^n p(\mu(z))p^\star(\mu(z^\star))$, which is clearly a real polynomial. If, moreover, $p(z)$ is self-conjugate, then we get that $Q(z) = \epsilon^{-1}(z^2+1)^n p(\mu(z))p(\mu^\star(z^\star))$. But it follows from (2.1) that $\mu^\star(z^\star) = 1/\mu(z) = \mu(-z)$, so that we obtain $Q(z) = \epsilon^{-1}(z^2+1)^n p(\mu(z))p\,(\mu(-z))$. Thus, we plainly see that $Q(-z) = Q(z)$, from which we conclude that $Q(z)$ has only even powers of z. □

Hence, provided that $z = 0$ is not a zero of $q_\mu(z)$ – which is the same of saying that $z = -1$ is not a zero of $p(z)$ – the number of real zeros of $q_\mu(z)$ will be twice the number of the positive zeros of $Q\left(\sqrt{z}\right)$, counted without multiplicity. This property allows us to modify Algorithm 1A by replacing $Q(z)$ with $Q\left(\sqrt{z}\right)$ and the procedure $\textsc{rrc}[Q(z), -\infty, \infty]$ with $2\,\textsc{rrc}[Q\left(\sqrt{z}\right), 0, \infty]$, so that a faster algorithm for self-conjugate polynomials is achieved (because now $Q\left(\sqrt{z}\right)$ has degree n instead of $2n$). Notice, however, that the eventual zero of $p(z)$ at $z = -1$ should be counted separately, in the same fashion as the eventual zero of $p(z)$ at the point $z = 1$. This is exemplified in Algorithm 3. We should remark, however, that this algorithm is not suitable for counting the number of zeros that a self-conjugate polynomial $p(z)$ of degree n has in a finite interval $\mathcal{J} = (e^{i\alpha}, e^{i\beta}]$ of $\mathbb{S}$ because the change of variable $z \leftarrow \sqrt{z}$ is not a one-to-one map. In fact, in this case we can no longer guarantee that the number of zeros that $Q(z)$ has on this interval corresponds to the twice the number of zeros of $Q(\sqrt{z})$ in the respective positive interval of the real line.

The another possibility is to define $Q(z)$ through $Q(z) = \textsc{gcd}\left[\frac{1}{2}\left(q_\mu(z) + q^\star_\mu(z^\star)\right), \frac{1}{2i}\left(q_\mu(z) - q^\star_\mu(z^\star)\right)\right]$. This has the advantage of providing a real polynomial $Q(z)$ whose degree is at most n. In fact, we have the following:

Theorem 7. *Let $p(z)$ be a self-conjugate polynomial of degree n. Then, the degree of the polynomial $Q(z) = \textsc{gcd}\left[\frac{1}{2}\left(q_\mu(z) + q^\star_\mu(z^\star)\right), \frac{1}{2i}\left(q_\mu(z) - q^\star_\mu(z^\star)\right)\right]$ will match the number of zeros of $p(z)$ that are symmetric to $\mathbb{S}$.*

Proof. We have seen in Theorems 3 and 4 that any pair of zeros of $p(z)$ that are on, or are symmetric to, the unit circle are mapped into a pair of real, or non-real complex conjugate, zeros of $q_\mu(z)$. On the other hand, Theorem 5 states that the zeros of the polynomial $Q(z)$ as defined above are precisely the complex conjugate zeros of $q_\mu(z)$. These two assertions imply that the degree of $Q(z)$ equals the number of zeros of $p(z)$ that are symmetric to $\mathbb{S}$. □

The corresponding algorithm is the same as Algorithm 1B and does not need to be presented again. We highlight, nevertheless, that if all the zeros of a self-conjugate polynomial $p(z)$ which not lie on $\mathbb{S}$ are not symmetric to $\mathbb{S}$ either, then the degree of $Q(z)$ provides directly the number of zeros of $p(z)$ on $\mathbb{S}$, so that in this case there is no need of using any RRC method whatsoever.

5. Self-inversive, self-adjoint and skew-adjoint polynomials

In this section we shall consider the case of a complex polynomial $p(z)$ whose zeros are all symmetric with respect to the unit circle. This means that, for any zero ζ of $p(z)$, the complex number $1/\zeta^\star$ is also a zero of it. Any polynomial of this kind is called a *self-inversive polynomial* and the necessary and sufficient condition for a polynomial $p(z) = p_n z^n + \cdots + p_0$ of degree n to be self-inversive is that $p_n p_0 \neq 0$ and that there exists a complex number ϵ with modulus 1 such that $p(z) = \epsilon z^n p^\star\left(1/z^\star\right)$ — see [24] for the proof. The coefficients of any self-inversive polynomial $p(z)$ of degree n satisfy the properties $p_{n-k} = \epsilon p^\star_k$, for k ranging from 0 to n. If a given polynomial is self-inversive with $\epsilon = 1$ (resp. $\epsilon = -1$) we shall call it a *self-adjoint* (*skew-adjoint*) *polynomial.*

The following theorem shows that there is a one-to-one correspondence between the sets of self-inversive and self-conjugate polynomials, as well as between the sets of self-adjoint and real polynomials.

Theorem 8. *Let $p(z)$ be a self-inversive polynomial. Then, the transformed polynomial $q_\mu(z)$ defined in (2.2) will be a self-conjugate polynomial. Moreover, if $p(z)$ is a self-adjoint (resp. skew-adjoint) polynomial, then the transformed polynomial $q_\mu(z)$ will be a real (imaginary) polynomial. Similarly, let $p(z)$ be a self-conjugate polynomial. Then the polynomial $q_\omega(z)$ defined in (2.2) will be a self-inversive polynomial and if $p(z)$ is a real (imaginary) polynomial, then $q_\omega(z)$ will be a self-adjoint (skew-adjoint) polynomial.*

Proof. The result follows from Theorems 3 and 4. Explicitly, we have the following: Let us first suppose $p(z)$ self-inversive. Then, $q_\mu(z) = (z+i)^n\, p(\mu(z)) = \epsilon\,(z+i)^n\, \mu(z)^n p^\star\left(1/\mu^\star(z)\right) = \epsilon\,(z-i)^n\, p^\star\left(1/\mu^\star(z)\right)$. But we have the identity

$1/\mu^\star(z) = \mu(z^\star)$, from which $q_\mu(z)$ simplifies to $q_\mu(z) = \epsilon\,(z-i)^n\,p^\star\left(\mu\left(z^\star\right)\right) = \epsilon q_\mu^\star(z^\star)$; this proves that $q_\mu(z)$ is self-conjugate. Besides, notice that if $\epsilon = 1$ (resp. $\epsilon = -1$), so that $p(z)$ is self-adjoint (skew-adjoint) polynomial, then we get that $q_\mu(z)$ will be a real (imaginary) polynomial because the value of ϵ is preserved during this transformation. Now, suppose $p(z)$ a self-conjugate polynomial. Then, we get that $q_\omega(z) = \left(\frac{i}{2}\right)^n (z-1)^n\, p(\omega(z)) = \epsilon\,(z-1)^n\,p^\star(\omega^\star(z))$. But we have the identity $\omega^\star(z) = \omega(1/z^\star)$, from which we obtain $q_\omega(z) = \epsilon\left(\frac{i}{2}\right)^n (z-1)^n\,p^\star\left(\omega\left(1/z^\star\right)\right) = \epsilon z^n q_\omega^\star\left(1/z^\star\right)$; this proves that $p(z)$ is self-inversive. Moreover, if $\epsilon = 1$ (resp. $\epsilon = -1$), so that $p(z)$ is a real (imaginary) polynomial, then we see that $q_\omega(z)$ becomes a self-adjoint (skew-adjoint) polynomial. □

Now, let us see how we can count the number of zeros that a self-adjoint or a self-inversive polynomial has on the unit circle. Let us first consider the case where $p(z)$ is self-adjoint. In this case, Theorem 8 ensures that $q_\mu(z)$ is already a real polynomial, so that there is no need of computing the polynomials $Q(z)$ introduced in Section 3. This results in Algorithm 4, which is usually faster than Algorithms 1A and 1B, as the steps concerning the computation of $Q(z)$ are absent. Of course, this algorithm also works for skew-adjoint polynomials: we just have to make the additional replacement $q_\mu(z) \leftarrow iq_\mu(z)$.

Algorithm 5: Self-inversive polynomials

input : A self-inversive polynomial $p(z)$ of degree n.
output: The number of distinct zeros of $p(z)$ on the unit circle.
$n :=$ degree$(p(z))$;
$\epsilon := p_n/p_0^\star$;
if $\epsilon \neq 1$ **then** $p(z) \leftarrow p\left(z\epsilon^{-1/n}\right)$ **end**;
$q(z) := (z+i)^n\, p\left(\frac{z-i}{z+i}\right)$;
$N :=$ RRC $[q(z), -\infty, \infty]$;
if $p(1) = 0$ **then** $N \leftarrow N+1$ **end**;
return N.

Algorithm 6: Self-reciprocal or skew-reciprocal polynomials

input : A self-reciprocal or skew-reciprocal polynomial $p(z)$ of degree n.
output: The number of distinct zeros of $p(z)$ on the unit circle.
$N := 0$;
if $p(1) = 0$ **then** $N \leftarrow N+1$ **end**;
if $p(-1) = 0$ **then** $N \leftarrow N+1$ **end**;
while $p(1) = 0$ **do** $p(z) \leftarrow \frac{p(z)}{z-1}$ **end**;
while $p(-1) = 0$ **do** $p(z) \leftarrow \frac{p(z)}{z+1}$ **end**;
$n :=$ degree$(p(z))$;
$q(z) := \left(\sqrt{z}+i\right)^n p\left(\frac{\sqrt{z}-i}{\sqrt{z}+i}\right)$;
$N \leftarrow N +$ RRC $[q(z), -\infty, \infty]$;
return N.

Let us now suppose $p(z)$ self-inversive with $\epsilon \neq 1$. In this case, the transformed polynomial $q_\mu(z)$ is not real anymore. A direct approach to work around this issue would be to compute the real polynomial $Q(z)$ as introduced in Section 3, but we actually have a better alternative: as the next theorem shows, a self-inversive polynomial $p(z)$ can always be transformed into a self-adjoint polynomial $s(z)$, whose degree is the same as that of $p(z)$, through a simple change of variable:

Theorem 9. *Let $p(z)$ be a self-inversive polynomial of degree n such that $\epsilon \neq 1$. Then, there exist n values for the real variable ϕ in the interval $0 < \phi \leqslant 2\pi$ for which the composition $s(z) = p(\mathrm{e}^{i\phi}z)$ will provide a self-adjoint polynomial of degree n. The possible values of ϕ are related with ϵ through the formula $\phi = (i\log\epsilon - 2\pi k)/n$, for $1 \leqslant k \leqslant n$, such that $\epsilon = \mathrm{e}^{-in\phi}$ for any admissible value of ϕ. Conversely, if $s(z)$ is a self-adjoint polynomial of degree n, then $p(z) = s\left(z\mathrm{e}^{-i\phi}\right)$ will provide a self-inversive polynomial of degree n such that $\epsilon = \mathrm{e}^{in\phi}$.*

Proof. Let $p(z) = p_n z^n + p_{n-1}z^{n-1} + \cdots + p_1 z + p_0$ be a self-inversive polynomial of degree n. Making the change of variable $z \leftarrow \mathrm{e}^{i\phi}z$, we shall get another polynomial of degree n, $s(z) = s_n z^n + s_{n-1}z^{n-1} + \cdots + s_1 z + s_0$, where $s_k = p_k \mathrm{e}^{ik\phi}$, $0 \leqslant k \leqslant n$. Now, $p(z)$ is self-inversive so that its coefficients satisfy the relations $p_{n-k} = \epsilon p_k^\star$, $0 \leqslant k \leqslant n$. From this we can see that the condition for $s(z)$ to be a self-adjoint polynomial is that $\epsilon = \mathrm{e}^{-in\phi}$. Inverting this relation, we conclude that ϕ can assume n distinct values in the interval $0 < \phi \leqslant 2\pi$, which are determined by the formula $\phi_k = (i\log\epsilon - 2\pi k)/n$, for $0 \leqslant k \leqslant n$; each one of them leads to a particular self-adjoint polynomial $s^{(k)}(z) = p\left(z\mathrm{e}^{i\phi_k}\right)$. Notice that, in terms of ϵ, we can also write: $s^{(k)}(z) = p\left(z\epsilon^{-1/n}/\varrho_n^k\right)$, $1 \leqslant k \leqslant n$, where $\varrho_n^k = e^{2\pi i \frac{k}{n}}$ denotes the kth root of unity of degree n. Finally, given a self-adjoint polynomial $s(z)$ of degree n, then it is clear that $p(z) = s(e^{-i\phi}z)$ will be a self-inversive polynomial with $\epsilon = e^{in\phi}$ for any admissible value ϕ_k of ϕ, as above. □

We highlight that Theorem 9 means that any self-inversive polynomial can be thought of a rotated self-adjoint polynomial. In fact, if $\zeta_1, \ldots, \zeta_n$ denote the zeros of a self-inversive polynomial $p(z)$ of degree n, and $\sigma_1^{(j)}, \ldots, \sigma_n^{(j)}$ the correspondent zeros of the self-adjoint polynomials $s^{(j)} = p(e^{i\phi_j})$, $1 \leqslant j \leqslant n$, as provided by Theorem 9, then it is a straightforward matter to show that $\sigma_k^{(j)} = e^{-i\phi_j}\zeta_k = \epsilon^{-1/n}\zeta_k/\varrho_n^j$, for any j and k running from 1 to n, where $\varrho_n^j = e^{2\pi i \frac{j}{n}}$. Therefore, we can say that the zeros of $s^{(j)}(z)$ are *rotated* with respect to the zeros of $p(z)$ by an angle equal to $\epsilon^{-1/n}/\varrho_n^j$ in the clockwise direction. Theorem 9 also shows us that if we rotate the zeros of a given self-inversive polynomial $p(z)$ of degree n by an angle equal to any root of unity of degree n, then we shall obtain another self-inversive polynomial with the same ϵ. This means there are exactly n self-inversive polynomials conjugated in this way for the same value of ϵ.

Now, Theorem 9 enables us to implement a specific algorithm for counting the number of zeros that a self-inversive polynomial has on $\mathbb{S}$. This is described in Algorithm 5. Because it differs from Algorithm 4 only by the replacement $p(z) \leftarrow p\left(ze^{-1/n}\right)$ (we can choose $\varrho_n^k = 1$), both algorithms have essentially the same complexity.

6. Self-reciprocal and skew-reciprocal polynomials. An application to Salem polynomials

As the last case to be discussed in this work, let us suppose the possibility of a complex polynomial $p(z)$ of degree n which is, at the same time, self-conjugate and self-inversive. From the properties $p(z) = \epsilon p^\star(z^\star)$ and $p(z) = z^n\epsilon p^\star(1/z^\star)$ which should be satisfied by self-conjugate and self-inversive polynomials, respectively, it follows that such polynomials should satisfy the property: $p(z) = \epsilon z^n p(1/z)$. Contrary to the previous cases, however, ϵ can assume only the values 1 or -1 (to see why, replace z by $1/z$ in the formula above), which means that $p(z)$ must be a real polynomial. In the first case ($\epsilon = 1$) we say that $p(z)$ is a *self-reciprocal polynomial*, while in the second case ($\epsilon = -1$), $p(z)$ is often called a *skew-reciprocal polynomial*. The coefficients of any self-reciprocal and any skew-reciprocal polynomial satisfy, respectively, the relations $p_{n-k} = p_k$ and $p_{n-k} = -p_k$, for any k from 0 to n, see [24].

The behaviour of self-reciprocal and skew-reciprocal polynomials at $z = \pm 1$ is described in the following

Theorem 10. *If $z = 1$ is a zero of a self-reciprocal polynomial $p(z)$, then its multiplicity is even. Moreover, if $z = -1$ is a zero of a self-reciprocal polynomial $p(z)$ of degree n, then its multiplicity is the same as the parity of n. Similarly, if $z = 1$ is a zero of a skew-reciprocal polynomial $p(z)$, then its multiplicity is odd. Moreover, if $z = -1$ is a zero of a skew-reciprocal polynomial $p(z)$ of degree n, then its multiplicity is the opposite of the parity of n.*

Proof. First of all, notice that any skew-reciprocal polynomial $p(z)$ has a zero at $z = 1$, as well as, any self-reciprocal (resp. skew-reciprocal) polynomial of odd (even) degree has a zero at $z = -1$. These propositions follow directly from the evaluation of $p(z)$ at $z = \pm 1$ and from the symmetry of its coefficients. Now, suppose that $z = 1$ is a zero of a self-reciprocal polynomial $p(z)$ of odd multiplicity, say $m = 2k + 1$, $k \in \mathbb{N}$. Then, $p(z) = (z-1)^{2k+1}P(z)$ and, as $(z-1)^{2k+1}$ is a skew-reciprocal polynomial, it follows that $P(z)$ would be a skew-reciprocal polynomial without zeros at $z = 1$, a contradiction. Similarly, suppose that $z = -1$ is a zero of $p(z)$ with multiplicity m. Then $p(z) = (z+1)^m P(z)$ and, as $(z+1)^m$ is self-reciprocal, it follows that $P(z)$ is self-reciprocal without zeros at $z = -1$. Thus $P(z)$ must have even degree, which implies that m has the same parity as the degree of $p(z)$. Moreover, suppose that $z = 1$ is a zero of a skew-reciprocal polynomial $p(z)$ of even parity, say, $m = 2k$, $k \in \mathbb{N}$. Then, $p(z) = (z-1)^{2k}P(z)$, and as $(z-1)^{2k}$ is self-reciprocal, it follows that $P(z)$ would be a skew-reciprocal polynomial without zeros at $z = 1$, again a contradiction. Similarly, suppose that $z = -1$ is a zero of $p(z)$ with multiplicity m. Then $p(z) = (z+1)^m P(z)$ and, as $(z+1)^m$ is self-reciprocal, it follows that $P(z)$ is skew-reciprocal without zeros at $z = -1$. Thus $P(z)$ must have odd degree, which implies that the parity of m is opposed to the parity of the degree of $p(z)$. □

Besides, the action of the Cayley transformation (2.1) over a self-reciprocal or skew-reciprocal polynomial $p(z)$ of degree n and with no zeros at $z = \pm 1$ leads to a real polynomial $q_\mu(z)$ of degree n in the variable z^2, as it is shown in the next theorem:

Theorem 11. *Let $p(z)$ be a self-reciprocal polynomial of even degree, say $n = 2m$, with no zeros at $z = \pm 1$. Then, the Cayley-transformed polynomial $q_\mu(z)$ will be a real polynomial of degree m in the variable z^2.*

Proof. Let $p(z)$ be a self-reciprocal polynomial of even degree, say, $n = 2m$. Because the coefficients of any self-reciprocal polynomial satisfy the relations $p_{n-k} = p_k$, $0 \leqslant k \leqslant n$, it follows that $p(z)$ can be written as, $p(z) = p_m z^m + \sum_{k=0}^{m-1} p_k\left(z^{2m-k} + z^k\right) = z^m\left[p_m + \sum_{k=0}^{m-1} p_k\left(z^{m-k} + z^{k-m}\right)\right]$. On the other hand, the transformed polynomial $q_\mu(z)$ defined in (2.2) becomes, $q_\mu(z) = \left(z^2+1\right)^m p_m + \sum_{k=0}^{m-1} p_k\left(z^2+1\right)^k\left[(z+i)^{2m-2k} + (z-i)^{2m-2k}\right]$, after a simplification. Therefore, we can plainly see that $q_\mu(z)$ is an even function of z, which means that $q(z)$ is in fact a polynomial of degree m on the variable z^2. Furthermore, $q_\mu(z)$ is also a real polynomial because all the imaginary terms inside the brackets will cancel after we expand the binomials. □

We can also show through similar arguments that, if $p(z)$ is a skew-reciprocal polynomial with no zero at $z = -1$, then the transformed polynomial $q_\mu(z)$ will be a pure imaginary polynomial in the variable z^2. Notice as well that any zero of $p(z)$ at $z = 1$ is mapped to infinity, as we have seen, so that the degree of $q_\mu(z)$ will be less than the degree of $p(z)$ in this case; similarly, any zero of $p(z)$ at $z = -1$ is mapped to zero, so that $p(z)$ will be multiplied by some power of z in this case.

Theorems 10 and 11 provide a great improvement to the algorithms presented in the previous sections. In fact, to count the number of zeros that a self-reciprocal or skew-reciprocal polynomial $p(z)$ has on $\mathbb{S}$, we can first remove its zeros (if any) at the points $z = 1$ and $z = -1$ by dividing it successively by $z - 1$ and $z + 1$ so that a self-reciprocal polynomial $r(z)$, with no zeros at $z = \pm 1$ is obtained in place. Then, we can compute the Cayley-transformation of $r(z)$ and, thanks to Theorem 11, to make the replacement $z \leftarrow \sqrt{z}$, which provides a polynomial of the half of the degree of $r(z)$. The number of real zeros of $r(z)$ will, therefore, equal the number of zeros on $\mathbb{S}$ of $p(z)$, excepting its possible zeros at $z = \pm 1$, which can be verified separately. This is described in Algorithm 6.

Finally, notice that from Algorithm 6 we can easily test if a given polynomial is (or not is) a *Salem polynomial* without knowing explicitly its zeros. A Salem polynomial $p(z)$ is a monic, irreducible, self-reciprocal polynomial of degree $n \geqslant 4$ with integer coefficients, whose all but two zeros lie on the unit circle. Their two zeros not lying on $\mathbb{S}$ are necessarily real, positive and the reciprocal of each other. The greatest real zero of a Salem polynomial is called its *Salem number*, and if the value of this number is less than the *smallest Pisot number* $\varrho \approx 1.3247179$ (which corresponds to the unique real zero of the Pisot polynomial $p(z) = z^3 - z - 1$), then it is usually called a *small Salem number*.[10]. A *Pisot polynomial* is a monic, irreducible, non-self-reciprocal integer polynomial that has only one zero outside the unit circle, which is its Pisot number. Up to date there were found only 47 small Salem numbers,[11] the smallest one being the *Lehmer number* $\lambda \approx 1.1762808$, the greatest real zero of the polynomial $L(z) = z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1$ — see [29,30]. It is still an open problem to know if Lehmer's number λ is the smallest Salem number, or even if there exists a smallest Salem number after all. We highlight that Algorithm 6 provides a powerful tool to look for polynomials with small Salem numbers and, in a more general way, to search for polynomials with small Mahler measure. We in fact succeeded in reproducing all small Salem numbers known up to date with an improved form of Algorithm 6 running in a simple desktop computer. We intend to report a detailed analysis of these researches in the future.

Acknowledgements

The author thanks the Editor and Referees for their valuable suggestions. This work was supported by Coordination for the Improvement of Higher Education Personnel (CAPES).

References

[1] J.-C. Pont, F. Padovani, Collected Works of Charles François Sturm, Birkhäuser Verlag, 2009.
[2] A.G. Akritas, Elements of Computer Algebra with Applications, Vol. 3, Wiley New York, 1989.
[3] J.M. Thomas, Sturm's theorem for multiple roots, Natl. Math. Mag. 15 (8) (1941) 391–394, http://dx.doi.org/10.2307/3028551.
[4] J. Fourier, Sur l'usage du théorème de Descartes dans la recherche des limites des racines, Bull. Sci. Soc. Phil. Paris (1820) 156–165.
[5] A.J.H. Vincent, Mémoire sur la résolution des équations numériques, Mém. Soc. R. Sci. Agric. Arts Lille 1 (1834) 1–34.
[6] A.J.H. Vincent, Note sur la résolution des équations numériques, J. Math. Pures Appl. 1 (1) (1836) 341–372.
[7] F.-D. Budan, Nouvelle méthode pour la résolution des équations numériques d'un degré quelconque, Courcier, 1807.
[8] G.E. Collins, A.G. Akritas, Polynomial real root isolation using Descarte's rule of signs, in: Proceedings of the Third ACM Symposium on Symbolic and Algebraic Computation, ACM, 1976, pp. 272–275, http://dx.doi.org/10.1145/800205.806346.
[9] A.G. Akritas, A new method for polynomial real root isolation, in: Proceedings of the 16th Annual Southeast Regional Conference, ACM, 1978, pp. 39–43.
[10] A. Alesina, M. Galuzzi, Vincent's theorem from a modern point of view, Rend. Circ. Mat. Palermo 2 (suppl. 64) (2000) 179–191.
[11] F. Rouillier, P. Zimmermann, Efficient isolation of polynomial's real roots, J. Comput. Appl. Math. 162 (1) (2004) 33–50, http://dx.doi.org/10.1016/j.cam.2003.08.015.
[12] A. Akritas, A. Strzeboński, P. Vigklas, On the various bisection methods derived from Vincent's theorem, Serdica J. Comput. 2 (1) (2008) 89–104.
[13] M. Sagraloff, K. Mehlhorn, Computing real roots of real polynomials, J. Symbolic Comput. 73 (2016) 46–86, http://dx.doi.org/10.1016/j.jsc.2015.03.004.
[14] A. Kobel, F. Rouillier, M. Sagraloff, Computing real roots of real polynomials... and now for real!, in: Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation, ACM, 2016, pp. 303–310, http://dx.doi.org/10.1145/2930889.2930937.
[15] R.S. Vieira, On the number of roots of self-inversive polynomials on the complex unit circle, Ramanujan J. 42 (2) (2017) 363–369, http://dx.doi.org/10.1007/s11139-016-9804-2.
[16] L.W. Ehrlich, A modified Newton method for polynomials, Commun. ACM 10 (2) (1967) 107–108, http://dx.doi.org/10.1145/363067.363115.
[17] O. Aberth, Iteration methods for finding all zeros of a polynomial simultaneously, Math. Comp. 27 (122) (1973) 339–344, http://dx.doi.org/10.1090/S0025-5718-1973-0329236-7.
[18] H.S. Wilf, A global bisection algorithm for computing the zeros of polynomials in the complex plane, J. ACM 25 (3) (1978) 415–420, http://dx.doi.org/10.1145/322077.322084.

[10] Actually, a Salem number is often called small if it is less than 1.3, see [29,30]. We think, however, that our definition is more appropriate, as the value 1.3 is quite arbitrary, in contrast with the smallest Pisot number ϱ which naturally plays an important role in the field.

[11] Please notice, however, that with the alternative definition adopted here, the list of known small Salem numbers presented for instance in [29,30] would be increased by some few new entries.

[19] T. Mitsui, A graphical technique for nonlinear algebraic equations, Int. J. Comput. Math. 13 (3–4) (1983) 245–261, http://dx.doi.org/10.1080/00207168308803367.
[20] D.A. Bini, Numerical computation of polynomial zeros by means of Aberth's method, Numer. Algorithms 13 (2) (1996) 179–200, http://dx.doi.org/10.1007/BF02207694.
[21] M.C. Brunetto, D. Claudio, V. Trevisan, An algebraic algorithm to isolate complex polynomial zeros using Sturm sequences, Comput. Math. Appl. 39 (3–4) (2000) 95–105, http://dx.doi.org/10.1016/S0898-1221(99)00336-3.
[22] V.Y. Pan, Univariate polynomials: nearly optimal algorithms for numerical factorization and root-finding, J. Symbolic Comput. 33 (5) (2002) 701–733, http://dx.doi.org/10.1006/jsco.2002.0531.
[23] M. Eisermann, The fundamental theorem of algebra made effective: an elementary real-algebraic proof via Sturm chains, Amer. Math. Monthly 119 (9) (2012) 715–752, http://dx.doi.org/10.4169/amer.math.monthly.119.09.715.
[24] R.S. Vieira, Polynomials with symmetric zeros, in: Polynomials – Theory and Application, IntechOpen, 2019, pp. 1–19, http://dx.doi.org/10.5772/intechopen.82728.
[25] A. Kempner, On equations admitting roots of the form $e^{i\theta}$, Tohoku Math. J. (1) 10 (1916) 115–117.
[26] A. Kempner, On the complex roots of algebraic equations, Bull. Amer. Math. Soc. 41 (12) (1935) 809–843.
[27] K. Conrad, Roots on a circle, 2016, Expository note.
[28] A.G. Akritas, P.S. Vigklas, Counting the number of real roots in an interval with Vincent's theorem, Bull. Math. Soc. Sci. Math. Roumanie (2010) 201–211.
[29] D.W. Boyd, Small Salem numbers, Duke Math. J. 44 (2) (1977) 315–328, http://dx.doi.org/10.1215/S0012-7094-77-04413-1.
[30] M. Mossinghoff, Polynomials with small Mahler measure, Math. Comput. Am. Math. Soc. 67 (224) (1998) 1697–1705, http://dx.doi.org/10.1090/S0025-5718-98-01006-0.