Theorem of three circles in Coq

Julianna Zsidó

Abstract

The theorem of three circles in real algebraic geometry guarantees the termination and correctness of an algorithm of isolating real roots of a univariate polynomial. The main idea of its proof is to consider polynomials whose roots belong to a certain area of the complex plane delimited by straight lines. After applying a transformation involving inversion this area is mapped to an area delimited by circles. We provide a formalisation of this rather geometric proof in Ssreflect, an extension of the proof assistant Coq, providing versatile algebraic tools. They allow us to formalise the proof from an algebraic point of view.

1 Introduction

The theorem of three circles that is the subject of this paper is not to be confused with the Hadamard three circle theorem in complex analysis. Our area of interest is algorithmic real algebraic geometry, for which [BPR06] is our main reference hereinafter. Before stating the theorem of three circles, which is called as such in [BPR06], chapter 10, we first introduce some necessary vocabulary and notations.

Let us fix an open real interval (l, r) and consider the following three open discs of the complex plane, see figure 1:

- $\mathcal{C}_0$ the disc bound by the circle with diameter (l, r);

- $\mathcal{C}_1$ the disc bound by the circumcircle of the equilateral triangle with base (l, r) and whose vertices have non-negative imaginary parts;

- $\mathcal{C}_2$ the disc symmetric to $\mathcal{C}_1$ with respect to the real axis.

Next we give some intuitive elements of the theory of so–called *Bernstein polynomials* needed for the theorem of three circles. Bernstein polynomials are associated to a certain interval (a, b), and a degree n, see figure 2 for $(a, b) = (0, 1)$, $n = 3$ and $n = 4$. They form a basis of Π_n, the vector space of polynomials of degree at most n. Bernstein polynomials can be used to approximate continuous functions on (a, b). Moreover they provide the control points for Bezier curves, which play an important role in image manipulation programs for example.
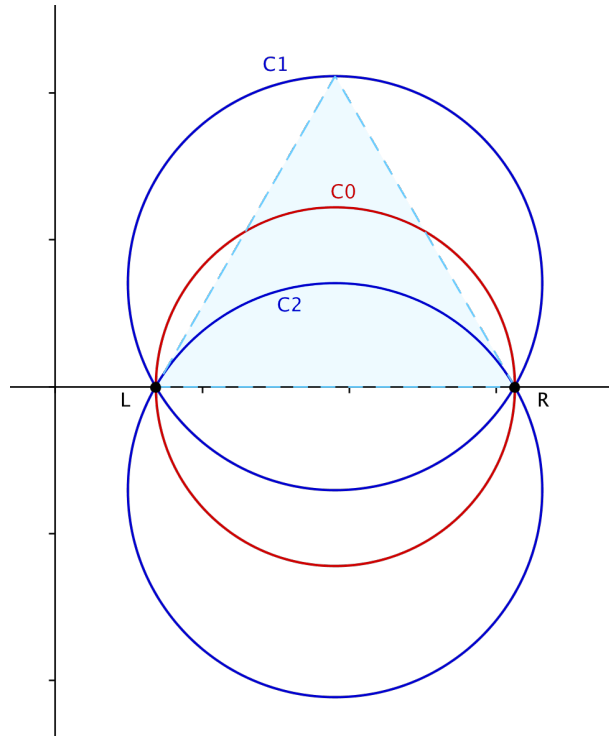
Figure 1: The delimiting circles of $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$
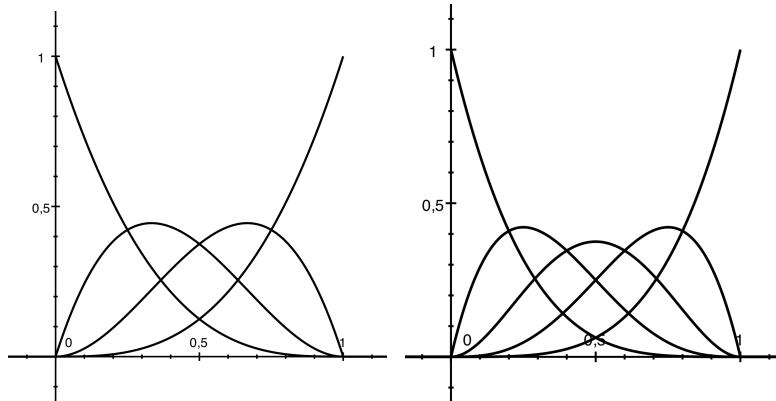

Figure 2: Bernstein polynomials for $n = 3$ and $n = 4$ on the interval $(0, 1)$

The coefficients of a polynomial expressed in the Bernstein basis are its *Bernstein cefficients*. In figure 2, we can see that the Bernstein polynomials have maxima in different points. So intuitively each Bernstein coefficient influences the behaviour of the polynomial in an interval around the maximum of the corresponding Bernstein polynomial. This does not mean that if a Bernstein coefficient is negative the polynomial is necessarily negative

on the interval under its influence, but under certain circumstances it can mean this.

The statement of the theorem of three circles is the following. Let P be a polynomial with real coefficients. If P has no roots in $\mathcal{C}_0$, then there is no variation of signs in the sequence of Bernstein coefficients of P. If P has exactly one simple root in the union $\mathcal{C}_1 \cup \mathcal{C}_2$, then there is exactly one variation of signs in the sequence of Bernstein coefficients of P.

This theorem is in a certain way reciprocal to Descartes' rule of signs, which states that the number of sign variations in the sequence of coefficients is an upper bound for the number of positive real roots (counted with multiplicities) and the difference of these two numbers is a multiple of 2. For the cases of sign variation 0 or 1, this rule implies the exact number of positive real roots.

The theorem of three circles guarantees the correctness and termination of the algorithm for real root isolation using Descartes' method, such as presented in [BPR06]. Since the algorithm bisects intervals in each iteration and then checks sign variations on the intervals, one possible terminating step would be similar to the one in figure 3.
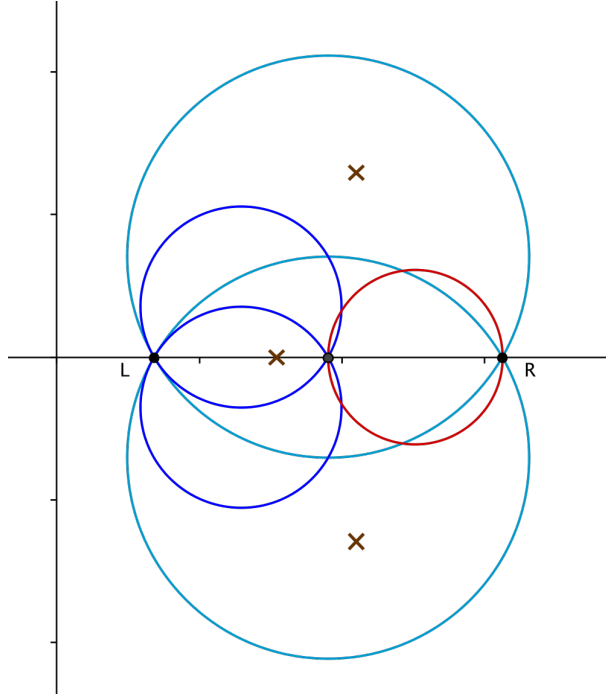

Figure 3: Three roots in the union of the large discs, only one real root in the union of the two small discs on the left

Algorithms for finding and separating real roots of polynomials play an important role in computer algebra, for example in the cylindrical algebraic

decomposition algorithm. Providing a formal proof of the cylindrical algebraic decomposition (CAD) algorithm has been an active field of research in the last decade, see for example works of A. Mahboubi [Mah06b], [Mah06a], [Mah07]. So our interest in formalising the theorem of three circles can be regarded as part of the efforts contributing to the formalisation of the CAD.

The CAD algorithm (due to G.E. Collins, developed in the 1970's) is an algorithm of quantifier elimination in real closed fields, and it represents at the same time an effective proof of one of Tarski's results from the 1950's, namely that the theory of real closed fields is decidable. The theory of real closed fields deals with polynomial equations and inequalities and roughly speaking describes real arithmetic. Decidability means here that the CAD is an algorithm that decides whether a given sentence in the first–order language of real closed fields is provable from the axioms of real closed fields. The algorithm is interesting on the one hand in real algebraic geometry when dealing with semialgebraic sets (sets described by polynomial inequalities) and on the other hand in mathematical logic since it provides an important theoretical result on real arithmetic. The CAD algorithm represents also an improvement of Tarski's historical algorithm from another point of view. Its complexity is double exponential whereas Tarski's algorithm has complexity of an exponential tower in the number of quantified variables. The research for complexity improvements of the CAD algorithm is still today an active field of research.

Recent developments in fast algorithms to isolate real roots of polynomials, in particular works of M. Sagraloff [MS09], [KS11], [Sag12], reinforced our motivations for formalising the theorem of three circles. The three disks $\mathcal{C}_0$, $\mathcal{C}_1$ and $\mathcal{C}_2$ represent two special cases of Obreshkoff areas. These areas are unions of open discs similar to $\mathcal{C}_1 \cup \mathcal{C}_2$, but whose centre points see the open interval (l, r) under the angle $\frac{2\pi}{k+2}$ for certain positive integers k. Obreshkoff lenses, which are intersections of the two discs similar to $\mathcal{C}_1$ and $\mathcal{C}_2$, together with the corresponding Obreshkoff areas play again a major role in proving the correctness and termination of the NewDsc algorithm [Sag12], which is an algorithm based on Descartes' method with Newton style iterations. So by formalising the special cases, we provide tools for the formalisation of the Obreshkoff areas and lenses (and an analogous theorem), which for their part are necessary for the formal verification of the NewDsc algorithm for example.

We chose to formalise the three circle theorem with the Ssreflect extension [Ssr] (whose name is derived from small-scale reflection) of Coq [CDT], since it provides versatile tools for dealing with algebraic structures and polynomials. An exhaustive introduction for Coq is for example Coq'Art, [BC04] and complementary technical details can be found in the Coq manual [CDT12]. Moreover [GM10] provides a nice introduction to Ssreflect. This work is supported by the European project ForMath [For].

2 Mathematical setting and prerequisites

The theorem of three circles is valid in any real closed field R, not only in the field of real numbers. The complex plane is replaced by the algebraic extension $C = R[i] = R[T]/(T^2 + 1)$ of R.

Moreover there is a certain number of prerequisite results which are needed for the theorem and its proof.

2.1 Bernstein coefficients

As we already mentioned in the introduction, the assertion of the theorem involves Bernstein coefficients, which are the coefficients of a given polynomial P of degree n in the Bernstein basis of the vector space Π_n of polynomials of degree at most n.

The Bernstein basis of Π_n consists of the Bernstein polynomials $B_{n,i,l,r}$, which are the defined on the open interval (l, r) as follows

$$B_{n,i,l,r}(X) = \binom{n}{i} \frac{(X - l)^i (r - X)^{n-i}}{(r - l)^n}$$

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

The Bernstein coefficients of a polynomial P can be computed from the coefficients of another polynomial Q which is obtained by applying a certain number of polynomial transformations on P. Before stating the corresponding proposition, we introduce the necessary transformations:

1. Translation by $c \in R$: $T_c(P(X)) = P(X - c)$,

2. Scaling by $c \in R$: $S_c(P(X)) = P(cX)$,

3. Inversion: $I_n(P(X)) = X^n P(1/X)$.

Proposition 2.1 ([BPR06]) *Let $P(X) = \sum_{i=0}^n b_i B_{n,i,l,r}(X)$ be a polynomial of $R[X]$ of degree at most n and let $Q(X) = T_{-1}(I_n(S_{r-l}(T_{-l}(P(X)))))$ whose coefficients (in the monomial basis) are denoted by c_i. Then $c_{n-i} = \binom{n}{i} b_i$.*

The proof of this proposition consists of the computation of the coefficients of Q.

Notation 2.2 *Inspired by [Eig08], we call the sequence of the above four transformations of the polynomial P a Möbius transformation of P; we will write $\mathrm{Mobius}(P)$ for the polynomial Q and call it the Möbius transform of P.*

2.2 Normal polynomials

Another ingredient in the proof of the theorem relies on results about so–called *normal* polynomials. A polynomial $P(X) = \sum_{i=0}^{p} a_i X^i$ is normal if and only if it satisfies the following conditions:

1. $0 \le a_i$ for all $i = 0, \ldots, p$;

2. $0 < a_p$;

3. $a_{i-1} a_{i+1} \le a_i^2$ for all $i = 0, \ldots, p$ (where coefficients with indices out of range are equal to 0);

4. for all $j \in \{0, \ldots, p\}$ such that $0 < a_j$ then $0 < a_i$ for all $i = j, \ldots, p$.

So we deal with polynomials whose sequence of coefficients consists of a certain number of zeros followed by positive ones up to the leading coefficient.

We have the following (almost immediate) consequences :

Lemma 2.3 ([BPR06]) *The polynomial $X - x$ is normal if and only if $x \le 0$.*

Lemma 2.4 ([BPR06]) *A second degree polynomial with a pair of complex conjugate roots is normal if and only if its roots are contained in the area $\mathcal{B} = \{a + bi \in R[i] \mid a \le 0, b^2 \le 3a^2\}$.*

Lemma 2.5 ([BPR06]) *The product of two normal polynomials is normal.*

The proofs of the first two lemmas are mainly computations. In the proof of the last one, one has to deal with double sums which are the coefficients of the product polynomial. It requires a tricky partition of the range of indices (or simply of $\mathbb{Z}^2$), the remaining part is technical but without any further difficulty.

With these three lemmas one can show the following proposition:

Proposition 2.6 ([BPR06]) *Let $P(X) \in R[X]$ be a monic polynomial. If all its roots belong to $\mathcal{B} = \{a + bi \in R[i] \mid a \le 0, b^2 \le 3a^2\}$, then P is normal.*

Remark 2.7 *Without loss of generality one can consider only normal polynomials whose sequence of coefficients does not contain zeros. Which is equivalent to considering only normal polynomials such that 0 is not a root, since the multiplicity of the root in 0 corresponds to the number of coefficients in the beginning of the sequence of coefficients.*

The main result involving normal polynomials is the following:

Proposition 2.8 ([BPR06]) *Let $P(X) \in R[X]$ be a normal polynomial and $0 < a$, then the number of sign variations in the sequence of coefficients of $P(X)(X - a)$ is exactly 1.*

Proof sketch. If we denote the coefficients of P by p_i and its degree by n, then we have

$$P(X)(X - a) = -p_0 a + p_1 \left(\frac{p_0}{p_1} - a \right) X + \ldots + p_n \left(\frac{p_{n-1}}{p_n} - a \right) X^n + p_n X^{n+1}$$

We have $-p_0 a < 0$ and $0 < p_n$, moreover the following chain of inequalities holds

$$\left(\frac{p_{k-1}}{p_k} - a \right) \leq \left(\frac{p_k}{p_{k+1}} - a \right)$$

for $k = 1, \ldots, n - 1$, because of the condition $p_{k-1} p_{k+1} \leq p_k^2$ for the normal polynomial P and the fact that all p_k are positive.

So the sequence of coefficients of $P(X)(X - a)$ without the first and the last elements has at most one sign change. If it has exactly one, $p_1 \left(\frac{p_0}{p_1} - a \right) \leq 0$ and $0 \leq p_n \left(\frac{p_{n-1}}{p_n} - a \right)$, so there is no sign change between the first and second or between the last and before last coefficients. If there is no sign change in the middle coefficients, $p_1 \left(\frac{p_0}{p_1} - a \right)$ and $p_n \left(\frac{p_{n-1}}{p_n} - a \right)$ have the same sign. If they are both negative, there is a sign change from $p_n \left(\frac{p_{n-1}}{p_n} - a \right)$ to p_n, if they are both positive, there is a sign change from $-p_0 a$ to $p_1 \left(\frac{p_0}{p_1} - a \right)$.

3 Using existing theories of Coq

In this section we are going to give some details on the previously formalised theories in Coq on which we base our proof on.

But first let us point out that the notation for functions $x \mapsto f(x)$ is written as fun x => f x in Coq.

We base our proof on the tools provided by the standard libraries of Ssreflect, developed by the Mathematical Components Project [Ssr], such as ssreflect, ssrbool, ssrnat, seq, path, poly, polydiv, ssralg and ssrnum. The latter two contain a hierarchy of algebraic structures, such as groups, rings, integral domains, fields, algebric fields, closed fields and their ordered counterparts. An exhaustive explanation of the organisation and formalisation of these structures can be found in section 2 of [CM12] or in chapters 2 and 4 of [Coh12].

Moreover we use less standard libraries, such as complex, polyorder, polyrcf, qe_rcf_th, pol and bern. We are going to explain the provided elements and notations of these libraries which are necessary to understand the codes shown in the next section.

In the following R denotes a real closed field, unless stated otherwise, and C = complex R its algebraic extension. The real part of a complex number z is denoted by Re z and its imaginary part by Im z.

The type {poly R} is provided for a ring R, representing the type of univariate polynomials with coefficients in R. The indeterminate X is written 'X, the k–th coefficient of the polynomial p is written p'_k, the composition of two polynomials p and q is written p \Po q and the degree of p is given by (size p).-1. The leading coefficient of p is written lead_coef p. We are using the predicate root p x which is true iff $p(x) = 0$, i.e. x is a root of p. Moreover p \is monic represents the predicate monic, so this expression is true iff the leading coefficient of p is equal to 1.

Polynomials are identified with the sequence of their coefficients. So indirectly, but often even directly, we deal with sequences when dealing with polynomials. The length of a sequence s is called size s and its i-th item is written s'_i. We are going to deal with the all and sorted constructions. The expression all a s is true iff the predicate a holds for each item of the sequence s. The expression sorted a s is true iff the binary relation a is true for each pair of consecutive items of s. Moreover we make some use of drop and take which are transformations of sequences, allowing to drop a certain number of items from the beginning of the sequence and to take a certain number of items starting from the beginning of the sequence (respectively). The filter operation on sequences comes handy too, filter a s is the sequence consisting of the items of s which satisfy the predicate a, its notation is [seq x <− s | (a x)], where the predicate is of the form fun x => a x. The mask operation is quite similar to filter, but it takes a boolean sequence b and another sequence s as inputs and returns the list consisting of items of s with all indices i for which b'_i = 1 holds. The operation zip takes two sequences as input and returns the sequence consisting of pairs of items, the first item in a pair from the first sequence, the second from the second sequence. The length of the "zipped list" is the length of the shorter input list. Mapping lists is done via map, it applies a given map point-wise to the items of the sequence. The notation for maps of lists is [seq (f x) | x <− s], where we apply fun x => f x to the items of s.

To talk about the number of sign changes in a sequence of elements of a real closed field, we use the function changes:

```
fun R : rcfType =>
fix changes (s : seq R) : nat :=
  match s with
  | nil => 0
  | a :: q => ((a ∗ head q < 0) + changes q)
  end.
```

by interpreting true as 1 and false as 0. This function cannot be used directly because it computes (for our purpose) erroneous values in the presence of

0 coefficients. It adds 1 to the count if $ab < 0$ if we write $[a, b, \ldots]$ for the sequence s. So for example changes $[:: -1; 0; 1]$ would yield 0 since $0 < 0$ is false. But in fact there is one sign change in the sequence $[-1, 0, 1]$, so we are going to use the function changes in combination with a filter that filters out the zeros from the sequence:

Definition seqn0 (s : seq R) := [seq x <− s | x ≠ 0].

Indeed changes (seqn0 $[::-1;0;1]$) yields 1. This definition of seqn0 as such is not provided by a library but it is rather a definition needed for our purposes and that complements changes.

A formal study of Bernstein coefficients has already been implemented, see [BGM11], the three transformations on polynomials and the Möbius transformation are provided by:

1. Translation by $-c$:

   Definition shift_poly (R : ringType) (c : R) (p : {poly R}) :=
      p \Po ('X + c).

   And its notation:

   Notation "p \shift c" := (shift_poly c p) (at level 50) : ring_scope.

2. Scaling by c:

   Definition scaleX_poly (R : ringType) (c : R) (p : {poly R}) :=
      p \Po ('X ∗ c).

   And its notation:

   Notation "p \scale c" := (scaleX_poly c p) (at level 50) : ring_scope.

3. Inversion:

   Definition reciprocal_pol (R : ringType) (p : {poly R}) :=
      \poly_(i < size p) p'_(size p − i.+1).

4. The Möbius transformation of $P(X)$ (from Proposition 2.1):

   Definition Mobius (R : ringType) (p : {poly R}) (a b : R) :=
      reciprocal_pol ((p \shift a) \scale (b − a)) \shift 1.

4   The proof of the theorem of three circles

The proof of the three circles theorem can be divided into two parts, since it actually consists of two assertions: the first one dealing with $\mathcal{C}_0$ and the second one with $\mathcal{C}_1 \cup \mathcal{C}_2$.

Remark 4.1 *Considering proposition 2.1, the number of sign changes in the sequence of Bernstein coefficients of a polynomial P is equal to the number of sign changes in the sequence of coefficients of the Möbius transformation* Mobius(P), *since reversing the sequence and multiplying each element by a positive number does not affect the number of sign changes.*

We point out the similar patterns in the proofs of the two parts. These similarities will be useful for the generalisation of the theorem we sketch in section 5.

1. First we have a statement about the number of sign changes in the sequence of the coefficients of a polynomial, whose roots belong to a certain area of the complex plane. This area is the half-plane of numbers with non-positive real parts in the first part and the corresponding statement is lemma 4.2. The area in the second part is $\mathcal{B}$ of lemma 2.4 and of proposition 2.6 and the statement about sign changes is proposition 2.8.

2. Then by the Möbius transformation of proposition 2.1, this area is transformed to another area of the complex plane: the exterior of the disc $\mathcal{C}_0$ in the first part and the exterior of $\mathcal{C}_1 \cup \mathcal{C}_2$ in the second part. See figures 4 and 5 for these transformations.

In the following subsections we are going to detail the proof of the theorem of three circles in three parts:

- Subsection 4.1 concerns the first assertion of the theorem involving $\mathcal{C}_0$, it contains both parts: before and after the Möbius transformation.

- Subsection 4.2 concerns the formalisation of the theory of normal polynomials as described in section 2.2. The goal of this section is to prove a statement about sign changes before the Möbius transformation.

- Finally subsection 4.3 concerns the second assertion of the theorem involving $\mathcal{C}_1 \cup \mathcal{C}_2$, its proof uses the theory of normal polynomials. This is what happens after the Möbius transformation.

4.1 First part of the proof: using polynomials with non-negative coefficients

We divide this subsection in two paragraphs: before and after the Möbius transformation.

4.1.1 Before the Möbius transformation

The goal of this paragraph is to prove the following lemma.

Lemma 4.2 *Let $P(X) \in R[X]$ be a monic polynomial. If all the roots of P have non-positive real parts, then there is no sign change in the sequence of coefficients of P.*

Proof sketch. This is actually a simple fact, that can be proven by induction on the degree of P.

If P has no roots, that is, if P is a constant polynomial, the assertion is obviously true. Let z be a root, so we can factor $P(X) = (X - z)P_1(X)$.

If z is real, then $z \leq 0$ by hypothesis, so $0 \leq -z$ and thus by multiplying out $(X - z)P_1(X)$, one obtains only non-negative coefficients. The sequence of only non-negative coefficients does not contain any sign changes.

If z has complex part different from 0, then $\overline{z}$ is a root as well and we can factor $P(X) = (X - z)(X - \overline{z})P_2(X) = (X^2 - 2\operatorname{Re}(z)X + \operatorname{Re}^2(z) + \operatorname{Im}^2(z))P_2(X)$. Since $\operatorname{Re}(z) \leq 0$, one obtains again only non-negative coefficients when multiplying out $(X^2 - 2\operatorname{Re}(z)X + \operatorname{Re}^2(z) + \operatorname{Im}^2(z))P_2(X)$.

In order to formalise this lemma, we first define a predicate nonneg using the provided predicate all; nonneg is true iff all items of a given sequence are non-negative:

Definition nonneg (s : seq R) := all (fun x => 0 ≤ x) s.

Then we prove the following lemmas representing elements of the above mentioned proof:

Lemma nonneg_poly_deg1 : $\forall$ (a : R),
    nonneg ('X − a) = (a ≤ 0).

Lemma nonneg_poly_deg2 : $\forall$ (z : C),
    nonneg ('X^2 − 2 (Re z) ∗ 'X + (Re z)^2 + (Im z)^2) = ((Re z) ≤ 0).

Lemma nonneg_mulr : $\forall$ (p q : {poly R}),
    (nonneg p) →
    (nonneg q) →
    nonneg (p ∗ q).

Lemma nonneg_root_nonpos : $\forall$ (p : {poly R}),
    (p \is monic) →
    ($\forall$ z : C, root p z → Re z ≤ 0) →
    nonneg p.

The proof of the last lemma is done by induction on the degree of p as in the proof sketch of Lemma 4.2. This formal proof contains the largest part of the sketched proof. The remaining two lemmas are almost immediate:

Lemma nonneg_changes0 : $\forall$ (s : seq R),
    (nonneg s) →
    changes s = 0.

Lemma monic_roots_changes_eq0 : $\forall$ (p : {poly R}),
   (p \is monic) $\rightarrow$
   ($\forall$ z : C, root p z $\rightarrow$ Re z $\leq$ 0) $\rightarrow$
   changes p = 0.

Having formalised the proof of lemma 4.2, we can now turn to the actual assertion of the theorem involving $\mathcal{C}_0$.

4.1.2 After the Möbius transformation

Explicitly the disc $\mathcal{C}_0$ is the area of $C = R[i]$ given by

$$\mathcal{C}_0 = \left\{ x + yi \in R[i] \mid \left(x - \frac{l+r}{2} \right)^2 + y^2 < \left(\frac{r-l}{2} \right)^2 \right\},$$

or equivalently by

$$\mathcal{C}_0 = \left\{ x + yi \in R[i] \mid x^2 - (l+r)x + y^2 + rl < 0 \right\}.$$

The condition on the roots is that they are in the complementary of $\mathcal{C}_0$, so we formalise directly the predicate:

Definition notinC (z : C) :=
   0 $\leq$ (Re z)^2 $-$ (l + r) $*$ (Re z) + (Im z)^2 + r $*$ l.

By using remark 4.1, the first part of the assertion is formalised as follows:

Theorem three_circles_1 : $\forall$ (p : {poly R}),
   ($\forall$ z : C, root p z $\rightarrow$ notinC z) $\rightarrow$
   changes (Mobius p l r) = 0.

As mentioned before, we want to use lemma 4.2 in this proof. In order to apply it, we have to make sure, that the polynomial we consider is monic. The polynomial (Mobius p l r) is in general not monic, but we can multiply it with the inverse of its leading coefficient and this operation does not affect the sign changes. This fact is formalised by:

Lemma changes_mulC : $\forall$ (p : {poly R}) (a : R),
   (a $\neq$ 0) $\rightarrow$
   changes p = changes (a $*$ p).

So now we can apply lemma monic_roots_changes_eq0, and it remains to prove that the roots of (Mobius p l r) all have non-positive real parts. Remembering that this latter polynomial is in fact Mobius$(P(X)) = T_{-1}(I_p(S_{r-l}(T_{-l}(P(X)))))$ whose roots all have non-positive real parts iff the roots of P are in the complement of $\mathcal{C}_0$. When keeping track of the roots during the four transformations, this is what happens: when translating by $-l$, and then scaling by $r - l$, the roots are "shifted" into the complement of the circle with diameter $(0, 1)$. By the following inversion, the complement

of the circle is mapped on the half–plane with real parts ≤ 1 and by translating this area by -1, we obtain the half–plane of numbers with non-positive real parts. See figure 4.
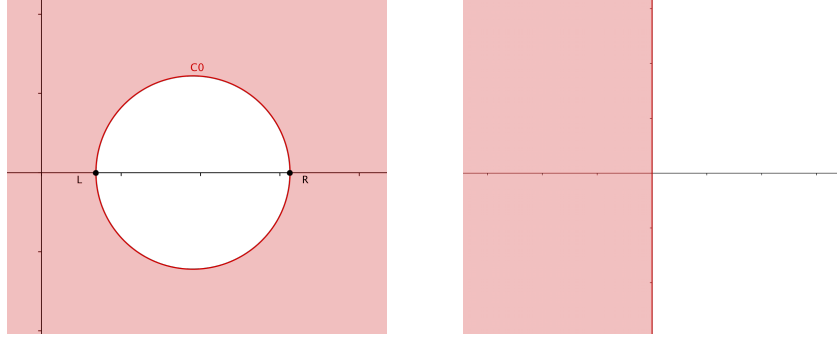

Figure 4: The Möbius transformation maps the exterior of $\mathcal{C}_0$ to the half-plane with non-positive real parts

This equivalence is not formalised as such, but is represented by the two lemmas:

Lemma root_Bernstein_coeffs_C_2 : $\forall$ (p : {poly R}) (z : C) (l r : R),
   (z + 1 $\neq$ 0) $\rightarrow$
   root p ((r + l $*$ z) / (z + 1)) = root (Mobius p l r) z.

and

Lemma notinC_Re_lt0_2 : $\forall$ (z : C), (z + 1 $\neq$ 0) $\rightarrow$
   (notinC ((r + l $*$ z) / (z + 1))) = (Re z $\leq$ 0).

One can see that when applying the above lemmas in the formal proof, the case of a root in $z = -1$ is excluded. In fact this case is treated separately, the assertion in this case can be shown directly since the real part of -1 is non-positive. This completes the formal proof of the first part of the theorem of three circles.

We see that the proof can be formalised basically the same way as the proof on paper suggests, thanks to all the existing theories and tools provided by the Ssreflect library.

4.2 Second part of the proof: formalising normal polynomials

This subsection contains the formalisation of subsection 2.2 about normal polynomials. The goal of this subsection is to prove a statement about sign changes before the Möbius transformation, proposition 2.8.

First we define recursively normal sequences:

Fixpoint normal_seq (s : seq R) :=

```
if s is (a::l1) then
    if l1 is (b::l2) then
        if l2 is (c::l3) then
            (normal_seq l1)
            && ((0 = a) || ((a * c ≤ b^2) && (0 < a) && (0 < b)))
        else (0 ≤ a) && (0 < b)
    else (0 < a)
else false.
```

Then we qualify a polynomial normal, if its sequence of coefficients is normal:

Definition normal := [qualify p : {poly R} | normal_seq p].

This definition allows us to write p \is normal hereinafter. Then we show several lemmas that guarantee that our definition of a normal polynomial agrees with the definition from section 2.2:

Lemma normal_coef_geq0 : ∀ (p : {poly R}),
  (p \is normal) →
  (∀ k, 0 ≤ p'_k).

Lemma normal_lead_coef_gt0 : ∀ (p : {poly R}),
  (p \is normal) →
  0 < lead_coef p.

Lemma normal_squares : ∀ (p : {poly R}),
  (p \is normal) →
  (∀ k, (1 ≤ k) → p'_(k.−1) * p'_(k.+1) ≤ p'_k^2).

Lemma normal_some_coef_gt0 : ∀ (p : {poly R}),
  (p \is normal) →
  (∀ i, (0 < p'_i) →
    (∀ j, (i < j) → (j < (size p).−1) → 0 < p'_j)).

Lemma prop_normal : ∀ (p : {poly R}),
  (∀ k, 0 ≤ p'_k) ∧
  (0 < lead_coef p) ∧
  (∀ k, (1 ≤ k) → p'_(k.−1) * p'_(k.+1) ≤ (p'_k)^2) ∧
  (∀ i, (0 < p'_i) →
    (∀ j, (i < j) → (j < (size p).−1) → 0 < p'_j)) →
  p \is normal.

Lemma 2.3 is formalised by:

Lemma monicXsubC_normal : ∀ (a : R),
  ('X − a) \is normal = (a ≤ 0).

The area $\mathcal{B}$ is defined by the following predicate:

14

Definition inB (z : C) :=
    (Re z ≤ 0) && ((Im z)^2 ≤3 ∗ (Re z)^2).

Lemma 2.4 is formalised by:

Lemma quad_monic_normal : ∀(z : C),
    (('X^2 − 2 ∗ (Re z) ∗ 'X + (Re z)^2 + (Im z)^2) \is normal) = (inB z).

The advantage of having formalised normal lists recursively is that in the proofs of monicXsubC_normal and quad_monic_normal the normal polynomials are computed by Coq automatically. Remark 2.7 is formalised by the lemma:

Lemma normal_0notroot : ∀(p : {poly R}),
    (p \is normal) →
    ∼(root p 0) ↔ ∀k, (k ≤(size p).−1) →0 < p'_k.

Lemma 2.5 is formalised by:

Lemma normal_mulr : ∀(p q : {poly R}),
    (p \is normal) →
    (q \is normal) →
    (p ∗ q) \is normal.

Its proof is done in several steps. First we formalise a restricted version where we have additional hypotheses on p and q: 0 is not a root of them. Then we prove that a polynomial P is normal if and only if $X^n P(X)$ is normal. Using this, one can factor out X^{μ_p} in p, X^{μ_q} in q and $X^{\mu_p + \mu_q}$ in their product and it suffices to show that $pq/X^{\mu_p + \mu_q}$ is normal.

Now we can formalise Proposition 2.6:

Lemma normal_root_inB : ∀(p : {poly R}),
    (p \is monic) →
    (∀z : C, root p z →inB z) →
    p \is normal.

Its proof is similar to the one of lemma nonneg_root_nonpos, it goes by induction on the degree of p. Let z be a root of p so that we can factor p= $(X − z)p_1(X)$. If z is real, then by hypothesis $z \leq 0$ and $(X − z)$ is normal by lemma 2.3. By induction hypothesis p_1 is normal. Since the product of two normal polynomials is normal we can conclude that p is normal. If z has non-zero imaginary part, then $\overline{z}$ is a root too and we can factor p=$(X − z)(X − \overline{z})p_2(X)$. By hypothesis $z \in \mathcal{B}$ and by symmetry $\overline{z} \in \mathcal{B}$ too. Thus $(X − z)(X − \overline{z})$ is normal by lemma 2.4. By induction hypothesis p_2 is normal. Since the product of two normal polynomials is normal, we can conclude that p is normal.

Recall from subsection 2.2 proposition 2.8: it states that the number of sign changes in the sequence of coefficients of $P(X)(X − a)$ is 1, where P is a normal polynomial and $a > 0$. The formalised proposition is as follows:

Lemma normal_changes : ∀ (a : R) (p : {poly R}),
   (0 < a) →
   (p \is normal) →
   (∼(root p 0)) →
   changes (seqn0 (p ∗ ('X − a))) = 1.

The hypothesis ∼(root p 0) is justified by remark 2.7. First we introduce the notation n = size (p ∗ ('X − a)).−1.

The formal proof of normal_changes is analogous to the sketched proof in subsection 2.2.

We prove first that $(p ∗ ('X − a))`\_0 < 0$ and that $0 < (p ∗ ('X − a))`\_n$ under the same hypotheses as the ones of normal_changes.

Then we continue by distinguishing two cases concerning the length of the sequence of coefficients of p ∗ ('X − a) (which is equivalent to distinguishing by the degree of this polynomial).

If the sequence consists of only two coefficients, then the assertion is immediately true. The sequence cannot consist of less coefficients since p, which is normal, cannot be the zero polynomial.

The main case is the one where the sequence consists of more than 2 coefficients. The proof of this case is analogous to the proof sketch of proposition 2.8 of subsection 2.2. In this case we can show that the number of sign changes can be decomposed into three terms:

- the number of sign changes between the first and second coefficients,

- the number of sign changes between the before last and last coefficients,

- the number of sign changes in the middle coefficients.

This decomposition is formalised by the following lemma:

Lemma changes_decomp_sizegt2 : ∀ (s : seq R),
   (all_neq0 s) →
   (2 < size s) →
   changes s = (s`_0 ∗ s`_1 < 0) + changes (mid s) +
          (s`_(size s).−2 ∗ s`_(size s).−1 < 0)

The predicate all_neq0 s is true iff all the items of s are different from 0 and the sequence mid s consists of s without the first and last items. We apply changes_decomp_sizegt2 to seqn0 (p ∗ ('X − a)).

Next we are going to simplify the number of sign changes in the middle coefficients of seqn0 (p ∗ ('X − a)). Recall from subsection 2.2 that the middle coefficients of (p ∗ ('X − a)) are of the form p`_k.+1 ∗ (p`_k / p`_k.+1 − a). This sequence can be characterised as the point-wise product of the two sequences (drop 1 p) and a sequence spseq. This latter sequence represents the expressions p`_k / p`_k.+1 − a and is formalised by

Definition spseq := [seq x.1 / x.2 − a | x <− zip p (drop 1 p)].

The point-wise product of two sequences is formalised by seqmul of type
seq R → seq R → seq R, which takes two sequences as input and returns a
sequence whose items are products of the corresponding items of the two
input lists. So the above mentioned characterisation is formalised by the
following lemma:

Lemma seqmul_spseq_dropp : mid (p ∗ ('X −a)) = seqmul spseq (drop 1 p).

Moreover we show that drop 1 p consists of positive items and spseq is
increasing, by using the predicates all_pos and increasing:

Lemma all_pos_dropp : all_pos (drop 1 p).

Lemma spseq_increasing : increasing spseq.

But since we apply the filter seqn0 on the sequence of the middle coef-
ficients, so that changes counts the sign changes correctly, we have to show
some technical details due to the filter.

- The filter seqn0 and mid commute under the condition that the first
  and last items of a sequence are different from zero.

  Lemma mid_seqn0_C : ∀ (s : seq R),
      (s'_0 ≠ 0) →
      (s'_(size s).−1 ≠ 0) →
      mid (seqn0 s) = seqn0 (mid s).

- When examining closely the expressions p'_k.+1 ∗ (p'_k / p'_k.+1 − a),
  we remark that

  $$p_{k+1}\left(\frac{p_k}{p_{k+1}} - a\right) = 0 \qquad \Leftrightarrow \qquad \frac{p_k}{p_{k+1}} - a = 0$$

  because $p_k > 0$ for all coefficients of P. So the items filtered out by
  seqn0 in mid(p ∗ ('X − a)) are exactly the ones filtered out by seqn0
  in spseq. This fact is formalised by the following lemma:

  Lemma mid_seqn0q_decomp : mid (seqn0 (p ∗ ('X − a))) =
      seqmul (seqn0 spseq)
              (mask [seq x ≠ 0 | x <− mid (p ∗ ('X − a))] (drop 1 p))

Furthermore, since (seqn0 spseq) is a subsequence of spseq, it is in-
creasing as well:

Lemma subspseq_increasing : increasing (seqn0 spseq).

and since mask [seq x ≠ 0 | x <− mid (p ∗ ('X − a))] (drop 1 p) is a sub-
sequence of drop 1 p, all its items are positive:

Lemma subp_all_pos :
    all_pos (mask [seq x ≠ 0 | x <− mid (p ∗ ('X − a))] (drop 1 p)).

- Now we are ready to simplify the number of changes in the middle coefficients. We use the simple fact that the number of sign changes in a point-wise product of two sequences, where one of the sequences consists of positive items is equal to the number of sign changes in the other sequence. This fact is given by the lemma

  Lemma changes_mult : $\forall$ (s c : seq R),
    (all_pos c) $\rightarrow$
    (size s = size c) $\rightarrow$
    changes (seqmul s c) = changes s.

Summarising the technical lemmas, we obtain that
changes (seqn0 (mid (p ∗ ('X − a)))) is equal to changes (seqn0 spseq).

Just like in the proof sketch of proposition 2.8 in section 2.2, we show then that seqn0 spseq has at most 1 sign change since it is increasing.

This fact is formalised for a general increasing sequence by the lemma:

Lemma changes_seq_incr : $\forall$ (s : seq R),
    (increasing s) $\rightarrow$
    (all_neq0 s) $\rightarrow$
    (changes s == 1) || (changes s == 0).

The conclusion of this lemma is a boolean expression, more precisely a boolean disjunction. The boolean disjunction is written || in Ssreflect and the boolean equality is denoted by ==.

Then we proceed by distinction of cases: either 1 or 0 sign changes in seqn0 spseq. We use the notation d = size (seqn0 (p ∗ ('X − a))).−1 (and thus d.−1 = size (seqn0 spseq)).

1. First case : changes (seqn0 spseq) = 1. This means that the first item has negative sign and the last one positive sign. This is formalised by the lemma

   Lemma changes_seq_incr_1 : $\forall$ (s : seq R),
       (1 < size s) $\rightarrow$
       (increasing s) $\rightarrow$
       (all_neq0 s) $\rightarrow$
       (changes s == 1) = (s'_0 < 0) && (0 < s'_((size s).−1)).

   The notations of this lemma might seem odd at first sight, since its conclusion is an equality = between to expressions containing another sort of equality ==. The Ssreflect libraries of Coq are based on manipulating boolean expressions rather than propositions where possible. The expression s'_0 < 0 for example, is true or false, so is effectively a boolean. The same is valid for 0 < s'_((size s).−1. The operator && is the boolean conjunction. On the left-hand side of the equality the

expression changes s == 1 is a boolean expression as well, since it uses boolean equality ==. So the conclusion of the lemma is an equality between boolean expressions.

Applying this lemma to seqn0 spseq, we obtain (seqn0 spseq)'_0 < 0 on the one hand which implies that
(seqn0 (p * ('X − a)))'_0 * (seqn0 (p * ('X − a)))'_1 < 0 is false.

On the other hand we have $0 <$ (seqn0 spseq)'_d.−2 which implies that
(seqn0 (p * ('X − a)))'_d.−1 * (seqn0 (p * ('X − a)))'_d < 0 is false.

So the count of changes according to changes_decomp_sizegt2 adds up to 1.

2. Second case : changes (seqn0 spseq) = 0. This means that the signs of the first and last items are the same. This is formalised by the lemma:

Lemma changes_seq_incr_0 : $\forall$ (s : seq R),
   (0 < size s) $\rightarrow$
   (increasing s) $\rightarrow$
   (all_neq0 s) $\rightarrow$
   ((changes s == 0) = (0 < s'_0 * s'_((size s).−1))).

Again, the assertion is an equality between boolean expressions.

So either $0 <$ (seqn0 spseq)'_0 and $0 <$ (seqn0 spseq)'_d.−2 or
(seqn0 spseq)'_0 < 0 and (seqn0 spseq)'_d.−2 < 0.
If both are positive, then

(seqn0 (p * ('X − a)))'_0 * (seqn0 (p * ('X − a)))'_1 < 0

is true and

(seqn0 (p * ('X − a)))'_d.−1 * (seqn0 (p * ('X − a)))'_d < 0

is false. If both are negative, then

(seqn0 (p * ('X − a)))'_0 * (seqn0 (p * ('X − a)))'_1 < 0

is false and

(seqn0 (p * ('X − a)))'_d.−1 * (seqn0 (p * ('X − a)))'_d < 0

is true.

So the count of changes according to changes_decomp_sizegt2 adds up to 1.

This completes the formal proof of proposition 2.8 or of normal_changes, as well as the theory on normal polynomials needed for the proof of the second part.

4.3 Second part of the proof: using normal polynomials

This subsection formalises the part of the proof of the second assertion of the theorem of three circles that comes after the Möbius transformation.

First we need to formalise the union of the two disks $\mathcal{C}_1 \cup \mathcal{C}_2$. They have following equations:

$$\left\{ x + yi \in R[i] \mid \left(x - \frac{l+r}{2}\right)^2 + \left(y \pm \frac{\sqrt{3}(r-l)}{6}\right)^2 < \frac{(r-l)^2}{3} \right\},$$

or equivalently

$$\left\{ x + yi \in R[i] \mid x^2 - (l+r)x + y^2 \pm \frac{\sqrt{3}}{3}(r-l)y + rl < 0 \right\}.$$

So the union is formalised by the following predicate:

Definition inC12 (l r : R) (z : C) :=
    ((Re z)^2 − (l + r) ∗ (Re z) + (Im z)^2 − (r − l) ∗ (Im z) / (sqrt 3) +
      l ∗ r < 0) ||
    ((Re z)^2 − (l + r) ∗ (Re z) + (Im z)^2 + (r − l) ∗ (Im z) / (sqrt 3) +
      l ∗ r < 0).

The second part of the theorem of three circles asserts that if P has exactly one simple root in $\mathcal{C}_1 \cup \mathcal{C}_2$, then there is exactly one sign variation in the sequence of Bernstein coefficients of P. So actually P is of the form $P(X) = (X - a)\widetilde{P}(X)$ where $a \in (l, r)$ and a is not a root of $\widetilde{P}$. This assertion is formalised as follows:

Theorem three_circles_2 : $\forall$ (l r : R) (p : {poly R}) (a : R),
    ($\sim$(root p r)) $\rightarrow$
    (l < a < r) $\rightarrow$
    ($\sim$(root p a)) $\rightarrow$
    ($\forall$ z : C, root p z $\rightarrow \sim$ (inC12 l r z)) $\rightarrow$
    changes (seqn0 (Mobius (p ∗ ('X − a)) l r)) = 1.

The only exotic hypothesis is the one asking for r not to be a root of $\widetilde{P}$. The reason for this is the fact that we restrict ourselves to the case that 0 is not a root of the normal polynomial Mobius($\widetilde{P}$) if we want to use proposition 2.8 or normal_changes for the proof. To ask 0 not to be a root of Mobius($\widetilde{P}$) is equivalent of asking of r not to be a root of $\widetilde{P}$.

In order to apply lemma normal_changes, first we need to put Mobius(p ∗ ('X − a)) in the form (Mobius p) ∗ ('X − b). First we show that multiplying the sequence by a non-zero constant, such as the inverse of the leading coefficient of Mobius (p ∗ ('X −a)), doesn't change the number of sign variations:

Lemma changes_mulC : $\forall$ (p : {poly R}) (a : R),
    (a $\neq$ 0) $\rightarrow$
    changes p = changes (a ∗ p).

Then we show that the Möbius transformation is compatible with the product of polynomials:

Lemma Bernstein_coeffsM : $\forall$ (p q : {poly R}) (l r : R),
   Mobius (p $*$ q) l r $=$ (Mobius p l r) $*$ (Mobius q l r).

And we can compute explicitly the coefficients of the Möbius transformation of a monic polynomial of degree 1:

Lemma Bernstein_coeffs_Xsubc_monic : $\forall$ (a l r : R),
   (l $\neq$ r) $\rightarrow$
   (l $\neq$ a) $\rightarrow$
   (lead_coef (Mobius ('X $-$ a) l r))^(-1) $*$ (Mobius ('X $-$ a) l r)
      $=$ 'X $+$ ((r $-$ a) / (l $-$ a)).

Now we can apply lemma normal_changes and it remains to show its hypotheses. The first hypothesis $\frac{r-a}{l-a} < 0$ can be shown easily since $l < a < r$.
   To show the hypothesis that

(lead_coef (Mobius p l r))^(-1) $*$ (Mobius p l r) \is normal,

we apply lemma normal_root_inB. This polynomial is obviously monic. In order to show that all the roots of (Mobius p l r) are in $\mathcal{B}$, we show that it is equivalent to ask that all the roots of p are in the exterior of $\mathcal{C}_1 \cup \mathcal{C}_2$. We use thus the following lemma

Lemma inB_notinC12 : $\forall$ (l r : R) (z : C),
   (l $\neq$ r) $\rightarrow$
   (z $+$ 1 $\neq$ 0) $\rightarrow$
   (inB z) $= \sim\sim$(inC12 l r ((r $+$ l $*$ z) / (z $+$ 1))).

together with lemma root_Bernstein_coeffs_C_2 from section 4.1. The conclusion of lemma inB_notinC12 is an equality of boolean expressions using the boolean negation, denoted by $\sim\sim$.
   So we have obtained the equivalence between "all roots of (Mobius p l r) are in $\mathcal{B}$" and "all roots of p are in the exterior of $\mathcal{C}_1 \cup \mathcal{C}_2$".
   What happens here is intuitively similar to section 4.1. We keep track of the complementary area of $\mathcal{C}_1 \cup \mathcal{C}_2$ when doing the Möbius transformation: translation by $-l$, then scaling by $r - l$, inversion and translation by -1.
   The computations are not as immediate as in section 4.1, but lemma inB_notinC12 proves the correctness. The case of a root in $z = -1$ has to be treated apart, but without any further difficulty. This concludes the formal proof of the second assertion.

5   Discussion and future work

First we would like to mention some technical remarks concerning the formalisation the way it was carried out.
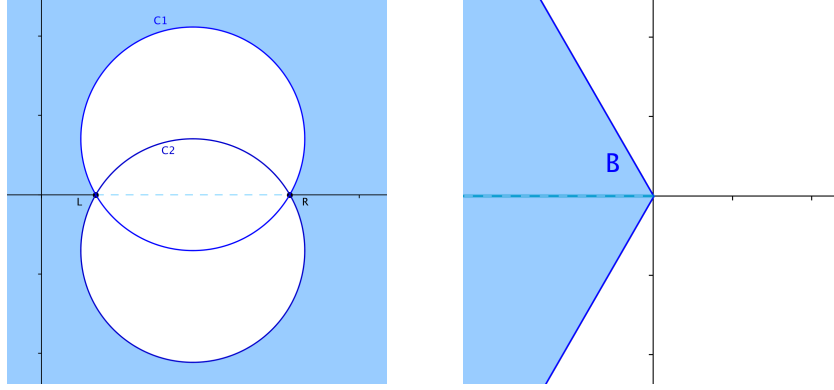
Figure 5: The Möbius transformation maps the exterior of $\mathcal{C}_1 \cup \mathcal{C}_2$ to the area $\mathcal{B}$

We implemented normal polynomials recursively because in the proofs of monicXsubC_normal and quad_monic_normal the computations are carried out automatically by Coq. Whereas in an alternative definition by a (rather cumbersome) predicate, one would have to show "by hand" the four defining properties. Another simplification of normal polynomials, considering remark 2.7, would have been to formalise only normal polynomials without any root in 0, since in almost all proofs thereafter, we add this hypothesis. We consider this simplification as part of our future work.

Another possibility of improving the proof is to develop apart a (small) theory of the function fun s : seq R => changes (seqn0 s) counting the sign changes in a sequence discarding the 0 items. It would make the proof more elegant, and the technical details such as the ones needed for the proof of normal_changes woud be treated in this theory and sourced out from the proof of the theorem of three circles.

As mentioned in the introduction, our main motivation for formalising the theorem of three circles is to formalise the general case involving Obreshkoff areas and lenses. Chapter two of [Eig08] explains all the details, presenting the relevant works of Obreshkoff. Lemmas nonneg_changes0 and 2.8, or its formalised version normal_changes, are generalised by the following theorem of Obreshkoff (restated in [Eig08] as Theorem 2.7)

Theorem 5.1 (Obreshkoff) *Consider the real polynomial*
$P(X) = \sum_{i=0}^{n} a_i X^i$ *of degree n and its complex roots, counted with multiplicities. Let v denote the number of sign changes of the sequence $(a_0, \ldots, a_n)$. If $P(X)$ has at least p roots with arguments in the range $-\frac{\pi}{n+2-p} < \varphi < \frac{\pi}{n+2-p}$, and at least $n - q$ roots with arguments in the range $\pi - \frac{\pi}{q+2} \leq \psi \leq \pi + \frac{\pi}{q+2}$, then $p \leq v \leq p$. If $p = q$, then $P(X)$ has exactly p roots with arguments φ in the range given above and $v = p$.*

The special case $p = q = 0$ is our lemma nonneg_changes0: the range for

ψ is $[\frac{\pi}{2}; \frac{3\pi}{2}]$, which corresponds to roots with non-positive real part.

The special case $p = q = 1$ is our lemma 2.8 or normal_changes: the range for ψ is $[\frac{2\pi}{3}; \frac{4\pi}{3}]$ which corresponds to the area $\mathcal{B}$ and one complex root (without its complex conjugate) with argument in the range $(-\frac{\pi}{n+1}; \frac{\pi}{n+1})$ implies that this root is in fact real and positive.

The transformation of polynomials from proposition 2.1 in order to obtain the Möbius transform or Mobius_p is characterised in [Eig08] as the Möbius transformation I of the interval $(0, \infty)$ to an arbitrary open interval (l, r):

$$P(X) \mapsto (X+1)^n P\left(\frac{r + lX}{X + 1}\right)$$

which is the transformation we use in lemma root_Bernstein_coeffs_C_2 (as well as in notinC_Re_lt0_2 and inB_notinC12). This is our reason for calling the sequence of the four transformations in proposition 2.1 a Möbius transformation.

The generalisation of the theorem of three circles is obtained by transferring theorem 5.1 to an arbitrary interval (l, r). To do so we define first Obreshkoff areas and lenses.

The two Obreshkoff discs $\overline{\mathcal{C}}_k$ and $\underline{\mathcal{C}}_k$ for an integer k are the open discs whose delimiting circles touch the endpoints of (l, r) and whose centers see the line segment (l, r) under the angle $\frac{2\pi}{k+2}$. The Obreshkoff area A_k is the union $\overline{\mathcal{C}}_k \cup \underline{\mathcal{C}}_k$ and the Obreshkoff lens L_k is the intersection $\overline{\mathcal{C}}_k \cap \underline{\mathcal{C}}_k$.

Theorem 5.2 (Obreshkoff) *Consider the real polynomial $P(X)$ of degree n and its roots in the complex plane, counted with multiplicities. Let v denote the number of sign changes in the sequence of coefficients of the Möbius transformation of P to the interval (l, r). If P has at least p roots in the Oreshkoff lens L_{n-p} and at most q roots in the Obreshkoff area A_q, then $p \le v \le q$.*

The assertions of the theorem of three circles are the special cases of $p = q = 0$ and $p = q = 1$.

In order to formalise these two theorems 5.1 and 5.2, one would have to make the following changes (at least) in the definitions of the structures needed for the proofs.

- Adapt the definition of the discs $\mathcal{C}_1$ and $\mathcal{C}_2$ to Obreshkoff areas with at least one integer parameter. Formalise Obreshkoff lenses.

- Adapt the definition of the area $\mathcal{B}$, with at least one more parameter, define the area corresponding to the angle range for φ.

- Adapt the definition of normal polynomial with respect to the parametrised version of $\mathcal{B}$. If possible keep recursive definition, in order to make computations automatic when possible.

To carry out the proof of theorem 5.1, one would have to prove first the special case $q = n$. This proof could be done in two steps: first an analogous lemma to normal_root_inB, with a proof by induction on the degree of the polynomial P, and then an analogous one to normal_changes which provides an upper bound for the number of sign changes rather than an exact number of changes. Then with this special case one can prove the general statement of theorem 5.1 by applying the special case to $P(X)$ and $P(-X)$.

To prove theorem 5.2, we need first the mentioned Möbius transformation. For this purpose lemma root_Bernstein_coeffs_C_2 together with a similar lemma to inB_notinC12 are mostly enough. The proof of theorem 5.2 would be then quite analogous to the one of three_circles_2.

Bearing in mind that our work provides tools for the formalisation of correctness of the NewDsc algorithm for example, we would have accomplished the first step in this direction. But until the completion of this goal, we still have many opportunities for exploration of formalisation of mathematical theories.

References

[BC04]   Yves Bertot and Pierre Castéran. *Interactive theorem proving and program development.* Texts in Theoretical Computer Science. An EATCS Series. Springer-Verlag, Berlin, 2004. Coq'Art: the calculus of inductive constructions, With a foreword by Gérard Huet and Christine Paulin-Mohring.

[BGM11]   Yves Bertot, Frédérique Guilhot, and Assia Mahboubi. A formal study of Bernstein coefficients and polynomials. *Mathematical Structures in Computer Science*, 21(4):731–761, 2011.

[BPR06]   Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, second edition, 2006.

[CDT]   The Coq Development Team. The Coq Proof Assistant. http://coq.inria.fr.

[CDT12]   The Coq Development Team. *The Coq Proof Assistant Reference Manual – Version V8.4*, 2012. http://coq.inria.fr.

[CM12]   Cyril Cohen and Assia Mahboubi. Formal proofs in real algebraic geometry: from ordered fields to quantifier elimination. *Logical Methods in Computer Science*, 8(1), 2012.

[Coh12]   Cytil Cohen. *Formalized algebraic numbers: construction and first order theory.* PhD thesis, École polytechnique, France, 2012.

[Eig08]   Arno Eigenwillig. *Real root isolation for exact and approximate polynomials using Descartes' rule of signs.* PhD thesis, Universität des Saarlandes, Germany, 2008.

[For]   ForMath. Thierry Coquand, project leader: The ForMath Project, EU FP7 STREP FET, grant agreement nr. 243847, March 2010 – February 2013. http://wiki.portal.chalmers.se/cse/pmwiki.php/ForMath/ForMath.

[GM10]   Georges Gonthier and Assia Mahboubi. An introduction to small scale reflection in Coq. *Journal of Formalized Reasoning*, 3(2):95–152, 2010.

[KS11]   Michael Kerber and Michael Sagraloff. Efficient real root approximation. In Éric Schost and Ioannis Z. Emiris, editors, *ISSAC*, pages 209–216. ACM, 2011.

[Mah06a] Assia Mahboubi. *Contributions à la certification des calculs dans R : théorie, preuves, programmation.* These, Université de Nice Sophia-Antipolis, Nov 2006.

[Mah06b] Assia Mahboubi. Programming and certifying a CAD algorithm in the Coq system. In *Dagstuhl Seminar 05021 - Mathematics, Algorithms, Proofs*, Dagstuhl, Germany, Jan 2006. Dagstuhl Online Research Publication Server.

[Mah07]   Assia Mahboubi. Implementing the cylindrical algebraic decomposition within the Coq system. *Math. Structures Comput. Sci.*, 17(1):99–127, 2007.

[MS09]   Kurt Mehlhorn and Michael Sagraloff. Isolating real roots of real polynomials. In Jeremy R. Johnson, Hyungju Park, and Erich Kaltofen, editors, *ISSAC*, pages 247–254. ACM, 2009.

[Sag12]   Michael Sagraloff. When Newton meets Descartes: a simple and fast algorithm to isolate the real roots of a polynomial. In Joris van der Hoeven and Mark van Hoeij, editors, *ISSAC*, pages 297–304. ACM, 2012.

[Ssr]   Ssreflect. The mathematical components project: Ssreflect extension and libraries. http://www.msr-inria.com/projects/mathematical-components.