

The Theorem of Three Circles

Fox Thomson, Wenda Li

March 17, 2025

Abstract

The Descartes test based on Bernstein coefficients and Descartes' rule of signs effectively (over-)approximates the number of real roots of a univariate polynomial over an interval. In this entry we formalise the theorem of three circles (Theorem 10.50 in [1]), which gives sufficient conditions for when the Descartes test returns 0 or 1. This is the first step for efficient root isolation.

Contents

1	Misc results about polynomials	2
1.1	Misc	2
1.2	Misc results about polynomials	3
1.3	The reciprocal polynomial	4
1.4	More about <i>proots-count</i>	7
1.5	More about <i>changes</i>	7
2	Bernstein Polynomials over the interval $[0, 1]$	8
2.1	Definition and basic results	9
2.2	<i>Bernstein-Poly-01</i> and <i>reciprocal-poly</i>	9
2.3	Bernstein coefficients and changes	10
2.4	Expression as a Bernstein sum	11
3	Bernstein Polynomials over any finite interval	12
3.1	Definition and relation to Bernstein Polynomials over $[0, 1]$.	12
3.2	Bernstein coefficients and changes over any interval	13
3.3	The control polygon of a polynomial	14
4	Normal Polynomials	14
5	Proof of the theorem of three circles	16
5.1	No sign changes case	17
5.2	One sign change case	18
5.3	The theorem of three circles	19

1 Misc results about polynomials

theory *RR1-Misc* **imports**

HOL-Computational-Algebra.Computational-Algebra

Budan-Fourier.BF-Misc

Polynomial-Interpolation.Ring-Hom-Poly

begin

1.1 Misc

declare *pcompose-pCons*[*simp del*]

lemma *Setcompr-subset*: $\bigwedge f P S. \{f x \mid x. P x\} \subseteq S = (\forall x. P x \longrightarrow f x \in S)$
 $\langle proof \rangle$

lemma *map-cong'*:

assumes $xs = \text{map } h \text{ } ys$ **and** $\bigwedge y. y \in \text{set } ys \implies f (h y) = g y$

shows $\text{map } f \text{ } xs = \text{map } g \text{ } ys$

$\langle proof \rangle$

lemma *nth-default-replicate-eq*:

$\text{nth-default } dftt (\text{replicate } n \text{ } x) \text{ } i = (\text{if } i < n \text{ then } x \text{ else } dftt)$

$\langle proof \rangle$

lemma *square-bounded-less*:

fixes $a b :: 'a :: \text{linordered-ring-strict}$

shows $-a < b \wedge b < a \implies b * b < a * a$

$\langle proof \rangle$

lemma *square-bounded-le*:

fixes $a b :: 'a :: \text{linordered-ring-strict}$

shows $-a \leq b \wedge b \leq a \implies b * b \leq a * a$

$\langle proof \rangle$

context *vector-space*

begin

lemma *card-le-dim-spanning*:

assumes $BV: B \subseteq V$

and $VB: V \subseteq \text{span } B$

and $fB: \text{finite } B$

and $dVB: \text{dim } V \geq \text{card } B$

shows *independent* B

$\langle proof \rangle$

end

1.2 Misc results about polynomials

lemma *smult-power*: $\text{smult } (x \hat{=} n) (p \hat{=} n) = \text{smult } x p \hat{=} n$
 $\langle \text{proof} \rangle$

lemma *reflect-poly-monom*: $\text{reflect-poly } (\text{monom } n \ i) = \text{monom } n \ 0$
 $\langle \text{proof} \rangle$

lemma *poly-eq-by-eval*:
fixes $P \ Q :: 'a :: \{\text{comm-ring-1}, \text{ring-no-zero-divisors}, \text{ring-char-0}\}$ *poly*
assumes $h: \bigwedge x. \text{poly } P \ x = \text{poly } Q \ x$ **shows** $P = Q$
 $\langle \text{proof} \rangle$

lemma *poly-binomial*:
 $[(1 :: 'a :: \text{comm-ring-1}), 1:] \hat{=} n = (\sum k \leq n. \text{monom } (\text{of-nat } (n \text{ choose } k)) \ k)$
 $\langle \text{proof} \rangle$

lemma *degree-0-iff*: $\text{degree } P = 0 \longleftrightarrow (\exists a. P = [:a:])$
 $\langle \text{proof} \rangle$

interpretation *poly-vs*: *vector-space smult*
 $\langle \text{proof} \rangle$

lemma *degree-subspace*: $\text{poly-vs.subspace } \{x. \text{degree } x \leq n\}$
 $\langle \text{proof} \rangle$

lemma *monom-span*:
 $\text{poly-vs.span } \{\text{monom } 1 \ x \mid x. x \leq p\} = \{(x :: 'a :: \text{field } \text{poly}). \text{degree } x \leq p\}$
(is ?L = ?R)
 $\langle \text{proof} \rangle$

lemma *monom-independent*:
 $\text{poly-vs.independent } \{\text{monom } (1 :: 'a :: \text{field}) \ x \mid x. x \leq p\}$
 $\langle \text{proof} \rangle$

lemma *dim-degree*: $\text{poly-vs.dim } \{x. \text{degree } x \leq n\} = n + 1$
 $\langle \text{proof} \rangle$

lemma *degree-div*:
fixes $p \ q :: ('a :: \text{idom-divide})$ *poly*
assumes $q \ \text{dvd} \ p$
shows $\text{degree } (p \ \text{div} \ q) = \text{degree } p - \text{degree } q$ $\langle \text{proof} \rangle$

lemma *lead-coeff-div*:
fixes $p \ q :: ('a :: \{\text{idom-divide}, \text{inverse}\})$ *poly*
assumes $q \ \text{dvd} \ p$
shows $\text{lead-coeff } (p \ \text{div} \ q) = \text{lead-coeff } p / \text{lead-coeff } q$ $\langle \text{proof} \rangle$

lemma *complex-poly-eq*:
 $r = \text{map-poly of-real } (\text{map-poly } \text{Re } r) + \text{smult } i \ (\text{map-poly of-real } (\text{map-poly } \text{Im } r))$

$r))$
 $\langle \text{proof} \rangle$

lemma *complex-poly-cong*:
 $(\text{map-poly } \text{Re } p = \text{map-poly } \text{Re } q \wedge \text{map-poly } \text{Im } p = \text{map-poly } \text{Im } q) = (p = q)$
 $\langle \text{proof} \rangle$

lemma *map-poly-Im-of-real*: $\text{map-poly } \text{Im } (\text{map-poly of-real } p) = 0$
 $\langle \text{proof} \rangle$

lemma *mult-map-poly-imp-map-poly*:
assumes $\text{map-poly complex-of-real } q = r * \text{map-poly complex-of-real } p$
 $p \neq 0$
shows $r = \text{map-poly complex-of-real } (\text{map-poly } \text{Re } r)$
 $\langle \text{proof} \rangle$

lemma *map-poly-dvd*:
fixes $p q :: \text{real poly}$
assumes $\text{hdvd} : \text{map-poly complex-of-real } p \text{ dvd } \text{map-poly complex-of-real } q$
 $q \neq 0$
shows $p \text{ dvd } q$
 $\langle \text{proof} \rangle$

lemma *div-poly-eq-0*:
fixes $p q :: ('a :: \text{idom-divide}) \text{ poly}$
assumes $q \text{ dvd } p \text{ poly } (p \text{ div } q) x = 0 \text{ } q \neq 0$
shows $\text{poly } p x = 0$
 $\langle \text{proof} \rangle$

lemma *poly-map-poly-of-real-cnj*:
 $\text{poly } (\text{map-poly of-real } p) (\text{cnj } z) = \text{cnj } (\text{poly } (\text{map-poly of-real } p) z)$
 $\langle \text{proof} \rangle$

An induction rule on real polynomials, if $P \neq 0$ then either $(X - x)|P$ or $(X - z)(X - \text{cnj } z)|P$, we induct by dividing by these polynomials.

lemma *real-poly-roots-induct*:
fixes $P :: \text{real poly} \Rightarrow \text{bool}$ **and** $p :: \text{real poly}$
assumes $\text{IH-real} : \bigwedge p x. P p \Longrightarrow P (p * [: -x, 1 :])$
and $\text{IH-complex} : \bigwedge p a b. b \neq 0 \Longrightarrow P p$
 $\Longrightarrow P (p * [: a*a + b*b, -2*a, 1 :])$
and $H0 : \bigwedge a. P [: a :]$
defines $d \equiv \text{degree } p$
shows $P p$
 $\langle \text{proof} \rangle$

1.3 The reciprocal polynomial

definition *reciprocal-poly* :: $\text{nat} \Rightarrow 'a :: \text{zero poly} \Rightarrow 'a \text{ poly}$
where $\text{reciprocal-poly } p P =$

$Poly\ (rev\ ((coeffs\ P)\ @\ (replicate\ (p - degree\ P)\ 0)))$

lemma *reciprocal-0*: *reciprocal-poly* $p\ 0 = 0$ $\langle proof \rangle$

lemma *reciprocal-1*: *reciprocal-poly* $p\ 1 = monom\ 1\ p$
 $\langle proof \rangle$

lemma *coeff-reciprocal*:
assumes $hi: i \leq p$ **and** $hP: degree\ P \leq p$
shows $coeff\ (reciprocal-poly\ p\ P)\ i = coeff\ P\ (p - i)$
 $\langle proof \rangle$

lemma *coeff-reciprocal-less*:
assumes $hn: p < i$ **and** $hP: degree\ P \leq p$
shows $coeff\ (reciprocal-poly\ p\ P)\ i = 0$
 $\langle proof \rangle$

lemma *reciprocal-monom*:
assumes $n \leq p$
shows $reciprocal-poly\ p\ (monom\ a\ n) = monom\ a\ (p-n)$
 $\langle proof \rangle$

lemma *reciprocal-degree*: *reciprocal-poly* $(degree\ P)\ P = reflect-poly\ P$
 $\langle proof \rangle$

lemma *degree-reciprocal*:
fixes $P :: ('a::zero)\ poly$
assumes $hP: degree\ P \leq p$
shows $degree\ (reciprocal-poly\ p\ P) \leq p$
 $\langle proof \rangle$

lemma *reciprocal-0-iff*:
assumes $hP: degree\ P \leq p$
shows $(reciprocal-poly\ p\ P = 0) = (P = 0)$
 $\langle proof \rangle$

lemma *poly-reciprocal*:
fixes $P :: ('a::field)\ poly$
assumes $hp: degree\ P \leq p$ **and** $hx: x \neq 0$
shows $poly\ (reciprocal-poly\ p\ P)\ x = x^p * (poly\ P\ (inverse\ x))$
 $\langle proof \rangle$

lemma *reciprocal-fcompose*:
fixes $P :: ('a::\{ring-char-0, field\})\ poly$
assumes $hP: degree\ P \leq p$
shows $reciprocal-poly\ p\ P = monom\ 1\ (p - degree\ P) * fcompose\ P\ 1\ [:0, 1:]$
 $\langle proof \rangle$

lemma *reciprocal-reciprocal*:

fixes $P :: 'a::\{\text{field}, \text{ring-char-0}\} \text{ poly}$
assumes $hP: \text{degree } P \leq p$
shows $\text{reciprocal-poly } p (\text{reciprocal-poly } p P) = P$
 $\langle \text{proof} \rangle$

lemma *reciprocal-smult*:
fixes $P :: 'a::\text{idom} \text{ poly}$
assumes $h: \text{degree } P \leq p$
shows $\text{reciprocal-poly } p (\text{smult } n P) = \text{smult } n (\text{reciprocal-poly } p P)$
 $\langle \text{proof} \rangle$

lemma *reciprocal-add*:
fixes $P Q :: 'a::\text{comm-semiring-0} \text{ poly}$
assumes $\text{degree } P \leq p$ **and** $\text{degree } Q \leq p$
shows $\text{reciprocal-poly } p (P + Q) = \text{reciprocal-poly } p P + \text{reciprocal-poly } p Q$
(is ?L = ?R)
 $\langle \text{proof} \rangle$

lemma *reciprocal-diff*:
fixes $P Q :: 'a::\text{comm-ring} \text{ poly}$
assumes $\text{degree } P \leq p$ **and** $\text{degree } Q \leq p$
shows $\text{reciprocal-poly } p (P - Q) = \text{reciprocal-poly } p P - \text{reciprocal-poly } p Q$
 $\langle \text{proof} \rangle$

lemma *reciprocal-sum*:
fixes $P :: 'a \Rightarrow 'b::\text{comm-semiring-0} \text{ poly}$
assumes $hP: \bigwedge k. \text{degree } (P k) \leq p$
shows $\text{reciprocal-poly } p (\sum k \in A. P k) = (\sum k \in A. \text{reciprocal-poly } p (P k))$
 $\langle \text{proof} \rangle$

lemma *reciprocal-mult*:
fixes $P Q :: 'a::\{\text{ring-char-0}, \text{field}\} \text{ poly}$
assumes $\text{degree } (P * Q) \leq p$
and $\text{degree } P \leq p$ **and** $\text{degree } Q \leq p$
shows $\text{monom } 1 p * \text{reciprocal-poly } p (P * Q) =$
 $\text{reciprocal-poly } p P * \text{reciprocal-poly } p Q$
 $\langle \text{proof} \rangle$

lemma *reciprocal-reflect-poly*:
fixes $P :: 'a::\{\text{ring-char-0}, \text{field}\} \text{ poly}$
assumes $hP: \text{degree } P \leq p$
shows $\text{reciprocal-poly } p P = \text{monom } 1 (p - \text{degree } P) * \text{reflect-poly } P$
 $\langle \text{proof} \rangle$

lemma *map-poly-reciprocal*:
assumes $\text{degree } P \leq p$ **and** $f 0 = 0$
shows $\text{map-poly } f (\text{reciprocal-poly } p P) = \text{reciprocal-poly } p (\text{map-poly } f P)$
 $\langle \text{proof} \rangle$

1.4 More about *roots-count*

lemma *roots-count-monom*:

assumes $0 \notin A$

shows *roots-count* (monom 1 d) A = 0

<proof>

lemma *roots-count-reciprocal*:

fixes $P::'a::\{\text{ring-char-0,field}\}$ poly

assumes hP : degree $P \leq p$ **and** $h0$: $P \neq 0$ **and** $h0'$: $0 \notin A$

shows *roots-count* (reciprocal-poly p P) A = *roots-count* P { x . inverse $x \in A$ }

<proof>

lemma *roots-count-reciprocal'*:

fixes $P::\text{real poly}$

assumes hP : degree $P \leq p$ **and** $h0$: $P \neq 0$

shows *roots-count* P { x . $0 < x \wedge x < 1$ } =

roots-count (reciprocal-poly p P) { x . $1 < x$ }

<proof>

lemma *roots-count-pos*:

assumes *roots-count* P S > 0

shows $\exists x \in S$. poly P x = 0

<proof>

lemma *roots-count-of-root-set*:

assumes $P \neq 0$ $R \subseteq S$ **and** $\bigwedge x. x \in R \implies \text{poly } P x = 0$

shows *roots-count* P S $\geq \text{card } R$

<proof>

lemma *roots-count-of-root*: **assumes** $P \neq 0$ $x \in S$ poly P x = 0

shows *roots-count* P S > 0

<proof>

1.5 More about *changes*

lemma *changes-nonneg*: $0 \leq \text{changes } xs$

<proof>

lemma *changes-replicate-0*: **shows** *changes* (replicate n 0) = 0

<proof>

lemma *changes-append-replicate-0*: *changes* (xs @ replicate n 0) = *changes* xs

<proof>

lemma *changes-scale-Cons*:

fixes $xs::\text{real list}$ **assumes** hs : $s > 0$

shows *changes* (s * x # xs) = *changes* (x # xs)

<proof>

lemma *changes-scale*:
fixes $xs::('a::linordered-idom) \text{ list}$
assumes $hs: \bigwedge i. i < n \implies s \ i > 0$ **and** $hn: \text{length } xs \leq n$
shows $\text{changes } [s \ i * (\text{nth-default } 0 \ xs \ i). \ i \leftarrow [0..<n]] = \text{changes } xs$
 $\langle \text{proof} \rangle$

lemma *changes-scale-const*: **fixes** $xs::'a::linordered-idom \text{ list}$
assumes $hs: s \neq 0$
shows $\text{changes } (\text{map } ((*) \ s) \ xs) = \text{changes } xs$
 $\langle \text{proof} \rangle$

lemma *changes-snoc*: **fixes** $xs::'a::linordered-idom \text{ list}$
shows $\text{changes } (xs \ @ \ [b, a]) = (\text{if } a * b < 0 \text{ then } 1 + \text{changes } (xs \ @ \ [b])$
 $\text{else if } b = 0 \text{ then } \text{changes } (xs \ @ \ [a]) \text{ else } \text{changes } (xs \ @ \ [b]))$
 $\langle \text{proof} \rangle$

lemma *changes-rev*: **fixes** $xs::'a::linordered-idom \text{ list}$
shows $\text{changes } (\text{rev } xs) = \text{changes } xs$
 $\langle \text{proof} \rangle$

lemma *changes-rev-about*: **fixes** $xs::'a::linordered-idom \text{ list}$
shows $\text{changes } (\text{replicate } (p - \text{length } xs) \ 0 \ @ \ \text{rev } xs) = \text{changes } xs$
 $\langle \text{proof} \rangle$

lemma *changes-add-between*:
assumes $a \leq x$ **and** $x \leq b$
shows $\text{changes } (as \ @ \ [a, b] \ @ \ bs) = \text{changes } (as \ @ \ [a, x, b] \ @ \ bs)$
 $\langle \text{proof} \rangle$

lemma *changes-all-nonneg*: **assumes** $\bigwedge i. \text{nth-default } 0 \ xs \ i \geq 0$ **shows** $\text{changes } xs = 0$
 $\langle \text{proof} \rangle$

lemma *changes-pCons*: $\text{changes } (\text{coeffs } (pCons \ 0 \ f)) = \text{changes } (\text{coeffs } f)$
 $\langle \text{proof} \rangle$

lemma *changes-increasing*:
assumes $\bigwedge i. i < \text{length } xs - 1 \implies xs \ ! \ (i + 1) \geq xs \ ! \ i$
and $\text{length } xs > 1$
and $hd \ xs < 0$
and $last \ xs > 0$
shows $\text{changes } xs = 1$
 $\langle \text{proof} \rangle$

end

2 Bernstein Polynomials over the interval $[0, 1]$

theory *Bernstein-01*

```

imports HOL-Computational-Algebra.Computational-Algebra
          Budan-Fourier.Budan-Fourier
          RRI-Misc
begin

```

The theorem of three circles is a statement about the Bernstein coefficients of a polynomial, the coefficients when a polynomial is expressed as a sum of Bernstein polynomials. These coefficients behave nicely under translations and rescaling and are the coefficients of a particular polynomial in the $[0, 1]$ case. We shall define the $[0, 1]$ case now and consider the general case later, deriving all the results by rescaling.

2.1 Definition and basic results

definition *Bernstein-Poly-01* :: $\text{nat} \Rightarrow \text{nat} \Rightarrow \text{real poly}$ **where**
 $\text{Bernstein-Poly-01 } j \ p = (\text{monom } (p \text{ choose } j) \ j)$
 $\quad * (\text{monom } 1 \ (p-j) \circ_p [:1, -1:])$

lemma *degree-Bernstein*:
assumes $hb: j \leq p$
shows $\text{degree } (\text{Bernstein-Poly-01 } j \ p) = p$
 $\langle \text{proof} \rangle$

lemma *coeff-gt*:
assumes $hb: j > p$
shows $\text{Bernstein-Poly-01 } j \ p = 0$
 $\langle \text{proof} \rangle$

lemma *degree-Bernstein-le*: $\text{degree } (\text{Bernstein-Poly-01 } j \ p) \leq p$
 $\langle \text{proof} \rangle$

lemma *poly-Bernstein-nonneg*:
assumes $x \geq 0$ **and** $1 \geq x$
shows $\text{poly } (\text{Bernstein-Poly-01 } j \ p) \ x \geq 0$
 $\langle \text{proof} \rangle$

lemma *Bernstein-symmetry*:
assumes $j \leq p$
shows $(\text{Bernstein-Poly-01 } j \ p) \circ_p [:1, -1:] = \text{Bernstein-Poly-01 } (p-j) \ p$
 $\langle \text{proof} \rangle$

2.2 Bernstein-Poly-01 and reciprocal-poly

lemma *Bernstein-reciprocal*:
 $\text{reciprocal-poly } p \ (\text{Bernstein-Poly-01 } i \ p)$
 $\quad = \text{smult } (p \text{ choose } i) \ ([: -1, 1:] \wedge (p-i))$
 $\langle \text{proof} \rangle$

lemma *Bernstein-reciprocal-translate*:

reciprocal-poly p (*Bernstein-Poly-01* i p) $\circ_p$ $[1, 1:] =$
monom (p choose i) $(p - i)$
 $\langle \text{proof} \rangle$

lemma *coeff-Bernstein-sum-01*: **fixes** $b::\text{nat} \Rightarrow \text{real}$ **assumes** $hi: p \geq i$
shows
coeff (*reciprocal-poly* p
 $(\sum x = 0..p. \text{smult } (b \ x) \ (\text{Bernstein-Poly-01 } x \ p)) \circ_p [1, 1:]$)
 $(p - i) = (p \text{ choose } i) * (b \ i)$ (**is** $?L = ?R$)
 $\langle \text{proof} \rangle$

lemma *Bernstein-sum-01*: **assumes** $hP: \text{degree } P \leq p$
shows
 $P = (\sum j = 0..p. \text{smult}$
 $(\text{inverse } (\text{real } (p \text{ choose } j))) *$
 $\text{coeff } (\text{reciprocal-poly } p \ P \circ_p [1, 1:]) \ (p-j))$
 $(\text{Bernstein-Poly-01 } j \ p))$
 $\langle \text{proof} \rangle$

lemma *Bernstein-Poly-01-span1*:
assumes $hP: \text{degree } P \leq p$
shows $P \in \text{poly-vs.span } \{\text{Bernstein-Poly-01 } x \ p \mid x. x \leq p\}$
 $\langle \text{proof} \rangle$

lemma *Bernstein-Poly-01-span*:
 $\text{poly-vs.span } \{\text{Bernstein-Poly-01 } x \ p \mid x. x \leq p\}$
 $= \{x. \text{degree } x \leq p\}$
 $\langle \text{proof} \rangle$

2.3 Bernstein coefficients and changes

definition *Bernstein-coeffs-01* $:: \text{nat} \Rightarrow \text{real poly} \Rightarrow \text{real list}$ **where**
Bernstein-coeffs-01 $p \ P =$
 $[(\text{inverse } (\text{real } (p \text{ choose } j))) *$
 $\text{coeff } (\text{reciprocal-poly } p \ P \circ_p [1, 1:]) \ (p-j)). j \leftarrow [0..<(p+1)]]$

lemma *length-Bernstein-coeffs-01*: $\text{length } (\text{Bernstein-coeffs-01 } p \ P) = p + 1$
 $\langle \text{proof} \rangle$

lemma *nth-default-Bernstein-coeffs-01*: **assumes** $\text{degree } P \leq p$
shows $\text{nth-default } 0 \ (\text{Bernstein-coeffs-01 } p \ P) \ i =$
 $\text{inverse } (p \text{ choose } i) * \text{coeff } (\text{reciprocal-poly } p \ P \circ_p [1, 1:]) \ (p-i)$
 $\langle \text{proof} \rangle$

lemma *Bernstein-coeffs-01-sum*: **assumes** $\text{degree } P \leq p$
shows $P = (\sum j = 0..p. \text{smult } (\text{nth-default } 0 \ (\text{Bernstein-coeffs-01 } p \ P) \ j)$
 $(\text{Bernstein-Poly-01 } j \ p))$
 $\langle \text{proof} \rangle$

definition *Bernstein-changes-01* :: *nat* $\Rightarrow$ *real poly* $\Rightarrow$ *int* **where**
Bernstein-changes-01 *p P* = *nat* (*changes* (*Bernstein-coeffs-01* *p P*))

lemma *Bernstein-changes-01-def'*:
Bernstein-changes-01 *p P* = *nat* (*changes* [(*inverse* (*real* (*p choose j*)) *
coeff (*reciprocal-poly* *p P* $\circ_p$ [:1, 1:])) (*p-j*)). *j* $\leftarrow$ [*0..<p + 1*]])
 <proof>

lemma *Bernstein-changes-01-eq-changes*:
assumes *hP*: *degree P* $\leq$ *p*
shows *Bernstein-changes-01* *p P* =
changes (*coeffs* ((*reciprocal-poly* *p P*) $\circ_p$ [:1, 1:]))
 <proof>

lemma *Bernstein-changes-01-test*: **fixes** *P*::*real poly*
assumes *hP*: *degree P* $\leq$ *p* **and** *h0*: *P* $\neq$ 0
shows *roots-count* *P* {*x*. 0 < *x* $\wedge$ *x* < 1} $\leq$ *Bernstein-changes-01* *p P* $\wedge$
even (*Bernstein-changes-01* *p P* - *roots-count* *P* {*x*. 0 < *x* $\wedge$ *x* < 1})
 <proof>

2.4 Expression as a Bernstein sum

lemma *Bernstein-coeffs-01-0*: *Bernstein-coeffs-01* *p* 0 = *replicate* (*p+1*) 0
 <proof>

lemma *Bernstein-coeffs-01-1*: *Bernstein-coeffs-01* *p* 1 = *replicate* (*p+1*) 1
 <proof>

lemma *Bernstein-coeffs-01-x*: **assumes** *p* $\neq$ 0
shows *Bernstein-coeffs-01* *p* (*monom* 1 1) = [*i/p*. *i* $\leftarrow$ [*0..<(p+1)*]]
 <proof>

lemma *Bernstein-coeffs-01-add*:
assumes *degree P* $\leq$ *p* **and** *degree Q* $\leq$ *p*
shows *nth-default* 0 (*Bernstein-coeffs-01* *p* (*P* + *Q*)) *i* =
nth-default 0 (*Bernstein-coeffs-01* *p P*) *i* +
nth-default 0 (*Bernstein-coeffs-01* *p Q*) *i*
 <proof>

lemma *Bernstein-coeffs-01-smult*:
assumes *degree P* $\leq$ *p*
shows *nth-default* 0 (*Bernstein-coeffs-01* *p* (*smult* *a P*)) *i* =
a * *nth-default* 0 (*Bernstein-coeffs-01* *p P*) *i*
 <proof>

end

3 Bernstein Polynomials over any finite interval

theory *Bernstein*
imports *Bernstein-01*
begin

3.1 Definition and relation to Bernstein Polynomials over $[0, 1]$

definition *Bernstein-Poly* :: *nat* $\Rightarrow$ *nat* $\Rightarrow$ *real* $\Rightarrow$ *real* $\Rightarrow$ *real poly* **where**

Bernstein-Poly *j p c d* = *smult* ((*p choose j*)/(*d - c*) $\wedge$ *p*)
 (((*monom 1 j*) $\circ_p$ $[-c, 1:]$) * (*monom 1 (p-j)* $\circ_p$ $[d, -1:]$))

lemma *Bernstein-Poly-altdef*:

assumes *c* $\neq$ *d* **and** *j* $\leq$ *p*

shows *Bernstein-Poly* *j p c d* = *smult* (*p choose j*)

($[-c/(d-c), 1/(d-c):] \wedge j * [d/(d-c), -1/(d-c):] \wedge (p-j)$)

(**is** ?*L* = ?*R*)

$\langle$ *proof* $\rangle$

lemma *Bernstein-Poly-nonneg*:

assumes *c* $\leq$ *x* **and** *x* $\leq$ *d*

shows *poly* (*Bernstein-Poly* *j p c d*) *x* $\geq$ 0

$\langle$ *proof* $\rangle$

lemma *Bernstein-Poly-01*: *Bernstein-Poly* *j p 0 1* = *Bernstein-Poly-01* *j p*

$\langle$ *proof* $\rangle$

lemma *Bernstein-Poly-rescale*:

assumes *a* $\neq$ *b*

shows *Bernstein-Poly* *j p c d* $\circ_p$ $[a, 1:]$ $\circ_p$ $[0, b-a:]$

= *Bernstein-Poly* *j p* ((*c-a*)/(*b-a*)) ((*d-a*)/(*b-a*))

(**is** ?*L* = ?*R*)

$\langle$ *proof* $\rangle$

lemma *Bernstein-Poly-rescale-01*:

assumes *c* $\neq$ *d*

shows *Bernstein-Poly* *j p c d* $\circ_p$ $[c, 1:]$ $\circ_p$ $[0, d-c:]$

= *Bernstein-Poly-01* *j p*

$\langle$ *proof* $\rangle$

lemma *Bernstein-Poly-eq-rescale-01*:

assumes *c* $\neq$ *d*

shows *Bernstein-Poly* *j p c d* = *Bernstein-Poly-01* *j p*

$\circ_p$ $[0, 1/(d-c):] \circ_p$ $[-c, 1:]$

$\langle$ *proof* $\rangle$

lemma *coeff-Bernstein-sum*:

fixes *b*::*nat* $\Rightarrow$ *real* **and** *p*::*nat* **and** *c* *d*::*real*

defines $P \equiv (\sum j = 0..p. (smult (b j) (Bernstein-Poly j p c d)))$
assumes $i \leq p$ **and** $c \neq d$
shows $coeff ((reciprocal-poly p (P \circ_p [:c, 1:]$
 $\circ_p [:0, d-c:]))) \circ_p [:1, 1:] (p - i) = (p \text{ choose } i) * (b i)$
 $\langle proof \rangle$

lemma *Bernstein-sum*:
assumes $c \neq d$ **and** $degree P \leq p$
shows $P = (\sum j = 0..p. smult (inverse (real (p \text{ choose } j)))$
 $* coeff (reciprocal-poly p (P \circ_p [:c, 1:] \circ_p [:0, d-c:]$
 $\circ_p [:1, 1:] (p-j)) (Bernstein-Poly j p c d))$
 $\langle proof \rangle$

lemma *Bernstein-Poly-span1*:
assumes $c \neq d$ **and** $degree P \leq p$
shows $P \in poly-vs.span \{Bernstein-Poly x p c d \mid x. x \leq p\}$
 $\langle proof \rangle$

lemma *Bernstein-Poly-span*:
assumes $c \neq d$
shows $poly-vs.span \{Bernstein-Poly x p c d \mid x. x \leq p\} = \{x. degree x \leq p\}$
 $\langle proof \rangle$

lemma *Bernstein-Poly-independent*: **assumes** $c \neq d$
shows $poly-vs.independent \{Bernstein-Poly x p c d \mid x. x \in \{..p\}\}$
 $\langle proof \rangle$

3.2 Bernstein coefficients and changes over any interval

definition *Bernstein-coeffs* ::
 $nat \Rightarrow real \Rightarrow real \Rightarrow real \Rightarrow real \Rightarrow real \text{ list where}$
 $Bernstein-coeffs p c d P =$
 $[(inverse (real (p \text{ choose } j))) *$
 $coeff (reciprocal-poly p (P \circ_p [:c, 1:] \circ_p [:0, d-c:] \circ_p [:1, 1:] (p-j))$
 $j \leftarrow [0..<(p+1)])]$

lemma *Bernstein-coeffs-eq-rescale*: **assumes** $c \neq d$
shows $Bernstein-coeffs p c d P = Bernstein-coeffs-01 p (P \circ_p [:c, 1:] \circ_p [:0,$
 $d-c:])$
 $\langle proof \rangle$

lemma *nth-default-Bernstein-coeffs*: **assumes** $degree P \leq p$
shows $nth-default 0 (Bernstein-coeffs p c d P) i =$
 $inverse (p \text{ choose } i) * coeff$
 $(reciprocal-poly p (P \circ_p [:c, 1:] \circ_p [:0, d-c:] \circ_p [:1, 1:] (p-i))$
 $\langle proof \rangle$

lemma *Bernstein-coeffs-sum*: **assumes** $c \neq d$ **and** hP : $degree P \leq p$
shows $P = (\sum j = 0..p. smult (nth-default 0 (Bernstein-coeffs p c d P) j)$

(Bernstein-Poly j p c d))
 <proof>

definition *Bernstein-changes* :: nat $\Rightarrow$ real $\Rightarrow$ real $\Rightarrow$ real poly $\Rightarrow$ int **where**
Bernstein-changes p c d P = nat (changes (Bernstein-coeffs p c d P))

lemma *Bernstein-changes-eq-rescale*: **assumes** $c \neq d$ **and** degree P $\leq$ p
shows *Bernstein-changes* p c d P =
Bernstein-changes-01 p (P $\circ_p$ [:c, 1:] $\circ_p$ [:0, d-c:])
 <proof>

This is related and mostly equivalent to previous Descartes test [3]

lemma *Bernstein-changes-test*:
fixes P::real poly
assumes degree P $\leq$ p **and** P $\neq$ 0 **and** $c < d$
shows roots-count P {x. $c < x \wedge x < d$ } $\leq$ *Bernstein-changes* p c d P $\wedge$
 even (Bernstein-changes p c d P - roots-count P {x. $c < x \wedge x < d$ })
 <proof>

3.3 The control polygon of a polynomial

definition *control-points* ::
 nat $\Rightarrow$ real $\Rightarrow$ real $\Rightarrow$ real poly $\Rightarrow$ (real $\times$ real) list
where
control-points p c d P =
 [(((real i)*d + (real (p - i))*c)/p,
 nth-default 0 (Bernstein-coeffs p c d P) i).
 i $\leftarrow$ [0.. $(p+1)$]]

lemma *line-above*:
fixes a b c d :: real **and** p :: nat **and** P :: real poly
assumes hline: $\bigwedge i. i \leq p \implies a * (((real i)*d + (real (p - i))*c)/p) + b \geq$
 nth-default 0 (Bernstein-coeffs p c d P) i
and hp: p $\neq$ 0 **and** hcd: $c \neq d$ **and** hP: degree P $\leq$ p
shows $\bigwedge x. c \leq x \implies x \leq d \implies a*x + b \geq$ poly P x
 <proof>

end

4 Normal Polynomials

theory *Normal-Poly*
imports *RRI-Misc*
begin

Here we define normal polynomials as defined in Basu, S., Pollack, R., Roy, M.-F.: Algorithms in Real Algebraic Geometry. Springer Berlin Heidelberg, Berlin, Heidelberg (2016).

definition *normal-poly* :: ('a::{comm-ring-1,ord}) *poly* $\Rightarrow$ *bool* **where**

normal-poly *p* $\equiv$

(*p* $\neq$ 0) $\wedge$
 $(\forall i. 0 \leq \text{coeff } p \ i) \wedge$
 $(\forall i. \text{coeff } p \ i * \text{coeff } p \ (i+2) \leq (\text{coeff } p \ (i+1))^2) \wedge$
 $(\forall i \ j \ k. i \leq j \longrightarrow j \leq k \longrightarrow 0 < \text{coeff } p \ i$
 $\longrightarrow 0 < \text{coeff } p \ k \longrightarrow 0 < \text{coeff } p \ j)$

lemma *normal-non-zero*: *normal-poly* *p* $\Longrightarrow p \neq 0$

<proof>

lemma *normal-coeff-nonneg*: *normal-poly* *p* $\Longrightarrow 0 \leq \text{coeff } p \ i$

<proof>

lemma *normal-poly-coeff-mult*:

normal-poly *p* $\Longrightarrow \text{coeff } p \ i * \text{coeff } p \ (i+2) \leq (\text{coeff } p \ (i+1))^2$

<proof>

lemma *normal-poly-pos-interval*:

normal-poly *p* $\Longrightarrow i \leq j \Longrightarrow j \leq k \Longrightarrow 0 < \text{coeff } p \ i \Longrightarrow 0 < \text{coeff } p \ k$
 $\Longrightarrow 0 < \text{coeff } p \ j$

<proof>

lemma *normal-polyI*:

assumes (*p* $\neq$ 0)

and ($\bigwedge i. 0 \leq \text{coeff } p \ i$)

and ($\bigwedge i. \text{coeff } p \ i * \text{coeff } p \ (i+2) \leq (\text{coeff } p \ (i+1))^2$)

and ($\bigwedge i \ j \ k. i \leq j \Longrightarrow j \leq k \Longrightarrow 0 < \text{coeff } p \ i \Longrightarrow 0 < \text{coeff } p \ k \Longrightarrow 0 <$

coeff } p \ j)

shows *normal-poly* *p*

<proof>

lemma *linear-normal-iff*:

fixes *x*::*real*

shows *normal-poly* $[-x, 1:] \longleftrightarrow x \leq 0$

<proof>

lemma *quadratic-normal-iff*:

fixes *z*::*complex*

shows *normal-poly* $[(\text{cmod } z)^2, -2 * \text{Re } z, 1:]$

$\longleftrightarrow \text{Re } z \leq 0 \wedge 4 * (\text{Re } z)^2 \geq (\text{cmod } z)^2$

<proof>

lemma *normal-of-no-zero-root*:

fixes *f*::*real poly*

assumes *hzero*: *poly* *f* 0 $\neq$ 0 **and** *hdeg*: *i* $\leq$ *degree* *f*

and *hnorm*: *normal-poly* *f*

shows $0 < \text{coeff } f \ i$

<proof>

```

lemma normal-divide-x:
  fixes f::real poly
  assumes hnorm: normal-poly (f*[:0,1:])
  shows normal-poly f
  ⟨proof⟩

lemma normal-mult-x:
  fixes f::real poly
  assumes hnorm: normal-poly f
  shows normal-poly (f * [:0, 1:])
  ⟨proof⟩

lemma normal-poly-general-coeff-mult:
  fixes f::real poly
  assumes normal-poly f and  $h \leq j$ 
  shows  $\text{coeff } f (h+1) * \text{coeff } f (j+1) \geq \text{coeff } f h * \text{coeff } f (j+2)$ 
  ⟨proof⟩

lemma normal-mult:
  fixes f g::real poly
  assumes hf: normal-poly f and hg: normal-poly g
  defines df  $\equiv$  degree f and dg  $\equiv$  degree g
  shows normal-poly (f*g)
  ⟨proof⟩

lemma normal-poly-of-roots:
  fixes p::real poly
  assumes  $\bigwedge z. \text{poly } (\text{map-poly } \text{complex-of-real } p) z = 0$ 
   $\implies \text{Re } z \leq 0 \wedge 4 * (\text{Re } z)^2 \geq (\text{cmod } z)^2$ 
  and lead-coeff p = 1
  shows normal-poly p
  ⟨proof⟩

lemma normal-changes:
  fixes f::real poly
  assumes hf: normal-poly f and hx:  $x > 0$ 
  defines df  $\equiv$  degree f
  shows changes (coeffs (f*[:−x,1:])) = 1
  ⟨proof⟩

```

end

5 Proof of the theorem of three circles

```

theory Three-Circles
  imports Bernstein Normal-Poly
begin

```

The theorem of three circles is a result in real algebraic geometry about the number of real roots in an interval. It says if the number of roots in certain circles in the complex plane are zero or one then the number of roots in the circles is equal to the sign changes of the Bernstein coefficients on that interval for which the circles intersect the real line. This can then be used to determine if an interval has a real root in the bisection procedure, which is more efficient than Descartes' rule of signs.

The proof here follows Theorem 10.50 in Basu, S., Pollack, R., Roy, M.-F.: Algorithms in Real Algebraic Geometry. Springer Berlin Heidelberg, Berlin, Heidelberg (2016).

This theorem has also been formalised in Coq [4]. The relationship between this theorem and root isolation has been elaborated in Eigenwillig's PhD thesis [2].

5.1 No sign changes case

declare *degree-pcompose*[*simp del*]

corollary *descartes-sign-zero*:

fixes *p::real poly*
assumes $\bigwedge x::\text{complex}. \text{poly} (\text{map-poly of-real } p) x = 0 \implies \text{Re } x \leq 0$
and *lead-coeff* *p* = 1
shows *coeff* *p* *i* ≥ 0
<proof>

definition *circle-01-diam* :: *complex set* **where**

circle-01-diam =
 $\{x. \text{cmod } (x - (\text{of-nat } 1 :: \text{complex})/(\text{of-nat } 2)) < (\text{real } 1)/(\text{real } 2)\}$

lemma *pos-real-map*:

$\{x::\text{complex}. 1 / x \in (\lambda x. x + 1) ' \{x. 0 < \text{Re } x\}\} = \text{circle-01-diam}$
<proof>

lemma *one-circle-01*: **fixes** *P::real poly* **assumes** *hP*: *degree* *P* $\leq p$ **and** *P* $\neq 0$

and *proots-count* (*map-poly of-real* *P*) *circle-01-diam* = 0

shows *Bernstein-changes-01* *p* *P* = 0

<proof>

definition *circle-diam* :: *real $\Rightarrow$ real $\Rightarrow$ complex set* **where**

circle-diam *l* *r* = $\{x. \text{cmod } ((x - l) - (r - l)/2) < (r - l)/2\}$

lemma *circle-diam-rescale*: **assumes** *l* < *r*

shows *circle-diam* *l* *r* = $(\lambda x. (x * (r - l) + l)) ' \text{circle-01-diam}$
<proof>

lemma *one-circle*: **fixes** *P::real poly* **assumes** *l* < *r*

and *proots-count* (*map-poly of-real* *P*) (*circle-diam* *l* *r*) = 0

and $P \neq 0$
and $\text{degree } P \leq p$
shows *Bernstein-changes* $p \ l \ r \ P = 0$
 $\langle \text{proof} \rangle$

5.2 One sign change case

definition *upper-circle-01* :: complex set **where**
 $\text{upper-circle-01} = \{x. \text{cmod } (x - (1/2 + \text{sqrt}(3)/6 * i)) < \text{sqrt } 3 / 3\}$

lemma *upper-circle-map*:
 $\{x::\text{complex}. 1 / x \in (\lambda x. x + 1) ' \{x. \text{Im } x < \text{sqrt } 3 * \text{Re } x\}\} = \text{upper-circle-01}$
 $\langle \text{proof} \rangle$

definition *lower-circle-01* :: complex set **where**
 $\text{lower-circle-01} = \{x. \text{cmod } (x - (1/2 - \text{sqrt}(3)/6 * i)) < \text{sqrt } 3 / 3\}$

lemma *cnj-upper-circle-01*: $\text{cnj } ' \text{upper-circle-01} = \text{lower-circle-01}$
 $\langle \text{proof} \rangle$

lemma *lower-circle-map*:
 $\{x::\text{complex}. 1 / x \in (\lambda x. x + 1) ' \{x. \text{Im } x > -\text{sqrt } 3 * \text{Re } x\}\} = \text{lower-circle-01}$
 $\langle \text{proof} \rangle$

lemma *two-circles-01*:
fixes $P::\text{real poly}$
assumes hP : $\text{degree } P \leq p$ **and** $hP0$: $P \neq 0$ **and** $hp0$: $p \neq 0$
and h : *roots-count* (*map-poly of-real* P)
 $(\text{upper-circle-01} \cup \text{lower-circle-01}) = 1$
shows *Bernstein-changes-01* $p \ P = 1$
 $\langle \text{proof} \rangle$

definition *upper-circle* :: $\text{real} \Rightarrow \text{real} \Rightarrow \text{complex set}$ **where**
 $\text{upper-circle } l \ r = \{x::\text{complex}.$
 $\text{cmod } ((x - \text{of-real } l) / (\text{of-real } (r - l)) - (1/2 + \text{of-real } (\text{sqrt}(3))/6 * i)) < \text{sqrt } 3 / 3\}$

lemma *upper-circle-rescale*: **assumes** $l < r$
shows $\text{upper-circle } l \ r = (\lambda x. (x * (r - l) + l)) ' \text{upper-circle-01}$
 $\langle \text{proof} \rangle$

definition *lower-circle* :: $\text{real} \Rightarrow \text{real} \Rightarrow \text{complex set}$ **where**
 $\text{lower-circle } l \ r = \{x::\text{complex}.$
 $\text{cmod } ((x - \text{of-real } l) / (\text{of-real } (r - l)) - (1/2 - \text{of-real } (\text{sqrt}(3))/6 * i)) < \text{sqrt } 3 / 3\}$

lemma *lower-circle-rescale*:
assumes $l < r$
shows $\text{lower-circle } l \ r = (\lambda x. (x * (r - l) + l)) ' \text{lower-circle-01}$

$\langle proof \rangle$

lemma *two-circles*:

fixes $P::real\ poly$ **and** $l\ r::real$

assumes $h_l r: l < r$

and $h_P: degree\ P \leq p$

and $h_{P0}: P \neq 0$

and $h_{p0}: p \neq 0$

and $h: roots-count\ (map-poly\ of-real\ P)$

$(upper-circle\ l\ r \cup lower-circle\ l\ r) = 1$

shows $Bernstein-changes\ p\ l\ r\ P = 1$

$\langle proof \rangle$

5.3 The theorem of three circles

theorem *three-circles*:

fixes $P::real\ poly$ **and** $l\ r::real$

assumes $l < r$

and $h_P: degree\ P \leq p$

and $h_{P0}: P \neq 0$

and $h_{p0}: p \neq 0$

shows $roots-count\ (map-poly\ of-real\ P)\ (circle-diam\ l\ r) = 0 \implies$

$Bernstein-changes\ p\ l\ r\ P = 0$

and $roots-count\ (map-poly\ of-real\ P)$

$(upper-circle\ l\ r \cup lower-circle\ l\ r) = 1 \implies$

$Bernstein-changes\ p\ l\ r\ P = 1$

$\langle proof \rangle$

end

6 Acknowledgements

The work has been jointly supported by the Cambridge Mathematics Placements (CMP) Programme and the ERC Advanced Grant ALEXANDRIA (Project GA 742178).

References

- [1] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
- [2] A. Eigenwillig. Real root isolation for exact and approximate polynomials using descartes’ rule of signs. 2008.
- [3] W. Li and L. C. Paulson. Counting polynomial roots in isabelle/hol: a formal proof of the budan–fourier theorem. In *Proceedings of the 8th*

ACM SIGPLAN International Conference on Certified Programs and Proofs, pages 52–64, 2019.

- [4] J. Zsidó. Theorem of three circles in coq. *Journal of automated reasoning*, 53(2):105–127, 2014.