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

theory *RRI-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*: $\bigwedge f\ P\ S.\ \{f\ x \mid x.\ P\ x\} \subseteq S = (\forall\ x.\ P\ x \longrightarrow f\ x \in S)$
⟨*proof*⟩

lemma *map-cong′*:
assumes $xs = map\ h\ ys$ **and** $\bigwedge y.\ y \in set\ ys \Longrightarrow f\ (h\ y) = g\ y$
shows $map\ f\ xs = map\ g\ ys$
⟨*proof*⟩

lemma *nth-default-replicate-eq*:
nth-default dflt (*replicate n x*) i = (*if* $i < n$ *then* x *else dflt*)
⟨*proof*⟩

lemma *square-bounded-less*:
fixes $a\ b$::′a :: *linordered-ring-strict*
shows $-a < b \land b < a \Longrightarrow b*b < a*a$
⟨*proof*⟩

lemma *square-bounded-le*:
fixes $a\ b$::′a :: *linordered-ring-strict*
shows $-a \le b \land b \le a \Longrightarrow b*b \le a*a$
⟨*proof*⟩

context *vector-space*
begin

lemma *card-le-dim-spanning*:
assumes *BV*: $B \subseteq V$
and *VB*: $V \subseteq$ *span* B
and *fB*: *finite* B
and *dVB*: *dim* $V \ge$ *card* B
shows *independent* B
⟨*proof*⟩

end

1.2 Misc results about polynomials

lemma *smult-power*: $smult\ (x\widehat{\ }n)\ (p\widehat{\ }n) = smult\ x\ p\ \widehat{\ }\ n$
⟨*proof*⟩

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

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

lemma *poly-binomial*:
$[:(1::'a::comm\text{-}ring\text{-}1),\ 1:]\widehat{\ }n = (\sum k{\le}n.\ monom\ (of\text{-}nat\ (n\ choose\ k))\ k)$
⟨*proof*⟩

lemma *degree-0-iff*: $degree\ P = 0 \longleftrightarrow (\exists\, a.\ P = [:a:])$
⟨*proof*⟩

interpretation *poly-vs*: *vector-space smult*
⟨*proof*⟩

lemma *degree-subspace*: $poly\text{-}vs.subspace\ \{x.\ degree\ x \le n\}$
⟨*proof*⟩

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

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

lemma *dim-degree*: $poly\text{-}vs.dim\ \{x.\ degree\ x \le n\} = n + 1$
⟨*proof*⟩

lemma *degree-div*:
fixes $p\ q$::($'a$::*idom-divide*) *poly*
assumes q *dvd* p
shows $degree\ (p\ div\ q) = degree\ p - degree\ q$ ⟨*proof*⟩

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

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

r))
⟨*proof*⟩

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

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

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

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

lemma *div-poly-eq-0*:
fixes $p\ q$::(*'a*::*idom-divide*) *poly*
assumes $q\ dvd\ p\ poly\ (p\ div\ q)\ x = 0\ q \neq 0$
shows $poly\ p\ x = 0$
⟨*proof*⟩

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

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

lemma *real-poly-roots-induct*:
fixes P::*real poly* $\Rightarrow$ *bool* **and** p::*real poly*
assumes *IH-real*: $\bigwedge p\ x.\ P\ p \Longrightarrow P\ (p * [:-x,\ 1:])$
and *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 $d \equiv degree\ p$
shows $P\ p$
⟨*proof*⟩

1.3 The reciprocal polynomial

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

Poly (*rev* ((*coeffs* *P*) @ (*replicate* (*p* − *degree* *P*) *0*)))

lemma *reciprocal-0*: *reciprocal-poly* *p* *0* = *0* ⟨*proof*⟩

lemma *reciprocal-1*: *reciprocal-poly* *p* *1* = *monom* *1* *p*
⟨*proof*⟩

lemma *coeff-reciprocal*:
assumes *hi*: *i* ≤ *p* **and** *hP*: *degree* *P* ≤ *p*
shows *coeff* (*reciprocal-poly* *p* *P*) *i* = *coeff* *P* (*p* − *i*)
⟨*proof*⟩

lemma *coeff-reciprocal-less*:
assumes *hn*: *p* < *i* **and** *hP*: *degree* *P* ≤ *p*
shows *coeff* (*reciprocal-poly* *p* *P*) *i* = *0*
⟨*proof*⟩

lemma *reciprocal-monom*:
assumes *n* ≤ *p*
shows *reciprocal-poly* *p* (*monom* *a* *n*) = *monom* *a* (*p*−*n*)
⟨*proof*⟩

lemma *reciprocal-degree*: *reciprocal-poly* (*degree* *P*) *P* = *reflect-poly* *P*
⟨*proof*⟩

lemma *degree-reciprocal*:
fixes *P* :: (*'a*::*zero*) *poly*
assumes *hP*: *degree* *P* ≤ *p*
shows *degree* (*reciprocal-poly* *p* *P*) ≤ *p*
⟨*proof*⟩

lemma *reciprocal-0-iff*:
assumes *hP*: *degree* *P* ≤ *p*
shows (*reciprocal-poly* *p* *P* = *0*) = (*P* = *0*)
⟨*proof*⟩

lemma *poly-reciprocal*:
fixes *P*::*'a*::*field* *poly*
assumes *hp*: *degree* *P* ≤ *p* **and** *hx*: *x* ≠ *0*
shows *poly* (*reciprocal-poly* *p* *P*) *x* = *x*^*p* ∗ (*poly* *P* (*inverse* *x*))
⟨*proof*⟩

lemma *reciprocal-fcompose*:
fixes *P*::(*'a*::{*ring-char-0*,*field*}) *poly*
assumes *hP*: *degree* *P* ≤ *p*
shows *reciprocal-poly* *p* *P* = *monom* *1* (*p* − *degree* *P*) ∗ *fcompose* *P* *1* [:*0*, *1*:]
⟨*proof*⟩

lemma *reciprocal-reciprocal*:

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

lemma *reciprocal-smult*:
fixes P :: $'a$::*idom poly*
assumes h: *degree* $P \leq p$
shows *reciprocal-poly* p (*smult* n P) = *smult* n (*reciprocal-poly* p P)
⟨*proof*⟩

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

lemma *reciprocal-diff*:
fixes P Q :: $'a$::*comm-ring poly*
assumes *degree* $P \leq p$ **and** *degree* $Q \leq p$
shows *reciprocal-poly* p (P − Q) = *reciprocal-poly* p P − *reciprocal-poly* p Q
⟨*proof*⟩

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

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

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

lemma *map-poly-reciprocal*:
assumes *degree* $P \leq p$ **and** f *0* = *0*
shows *map-poly* f (*reciprocal-poly* p P) = *reciprocal-poly* p (*map-poly* f P)
⟨*proof*⟩

1.4 More about *proots-count*

lemma *proots-count-monom*:
  assumes $0 \notin A$
  shows $\mathit{proots\text{-}count}\ (\mathit{monom}\ 1\ d)\ A = 0$
  ⟨*proof*⟩

lemma *proots-count-reciprocal*:
  fixes $P::'a::\{\mathit{ring\text{-}char\text{-}0},\mathit{field}\}\ \mathit{poly}$
  assumes hP: $\mathit{degree}\ P \leq p$ **and** $h0$: $P \neq 0$ **and** $h0'$: $0 \notin A$
  shows $\mathit{proots\text{-}count}\ (\mathit{reciprocal\text{-}poly}\ p\ P)\ A = \mathit{proots\text{-}count}\ P\ \{x.\ \mathit{inverse}\ x \in A\}$
⟨*proof*⟩

lemma *proots-count-reciprocal'*:
  fixes $P::\mathit{real}\ \mathit{poly}$
  assumes hP: $\mathit{degree}\ P \leq p$ **and** $h0$: $P \neq 0$
  shows $\mathit{proots\text{-}count}\ P\ \{x.\ 0 < x \wedge x < 1\} =$
    $\mathit{proots\text{-}count}\ (\mathit{reciprocal\text{-}poly}\ p\ P)\ \{x.\ 1 < x\}$
⟨*proof*⟩

lemma *proots-count-pos*:
  assumes $\mathit{proots\text{-}count}\ P\ S > 0$
  shows $\exists\, x \in S.\ \mathit{poly}\ P\ x = 0$
⟨*proof*⟩

lemma *proots-count-of-root-set*:
  assumes $P \neq 0\ R \subseteq S$ **and** $\bigwedge x.\ x{\in}R \Longrightarrow \mathit{poly}\ P\ x = 0$
  shows $\mathit{proots\text{-}count}\ P\ S \geq \mathit{card}\ R$
⟨*proof*⟩

lemma *proots-count-of-root*: **assumes** $P \neq 0\ x{\in}S\ \mathit{poly}\ P\ x = 0$
  shows $\mathit{proots\text{-}count}\ P\ S > 0$
  ⟨*proof*⟩

1.5 More about *changes*

lemma *changes-nonneg*: $0 \leq \mathit{changes}\ xs$
  ⟨*proof*⟩

lemma *changes-replicate-0*: **shows** $\mathit{changes}\ (\mathit{replicate}\ n\ 0) = 0$
  ⟨*proof*⟩

lemma *changes-append-replicate-0*: $\mathit{changes}\ (xs\ @\ \mathit{replicate}\ n\ 0) = \mathit{changes}\ xs$
⟨*proof*⟩

lemma *changes-scale-Cons*:
  fixes $xs::\ \mathit{real}\ \mathit{list}$ **assumes** hs: $s > 0$
  shows $\mathit{changes}\ (s * x\ \#\ xs) = \mathit{changes}\ (x\ \#\ xs)$
  ⟨*proof*⟩

lemma *changes-scale*:
fixes *xs*::('*a*::*linordered-idom*) *list*
assumes *hs*: $\bigwedge i.\ i < n \Longrightarrow s\ i > 0$ **and** *hn*: *length xs* $\leq n$
shows *changes* [*s i* ∗ (*nth-default 0 xs i*). *i* ← [*0*..<*n*]] = *changes xs*
⟨*proof*⟩

lemma *changes-scale-const*: **fixes** *xs*::'*a*::*linordered-idom list*
assumes *hs*: $s \neq 0$
shows *changes* (*map* ((∗) *s*) *xs*) = *changes xs*
⟨*proof*⟩

lemma *changes-snoc*: **fixes** *xs*::'*a*::*linordered-idom list*
shows *changes* (*xs* @ [*b*, *a*]) = (*if a* ∗ *b* < *0 then 1* + *changes* (*xs* @ [*b*])
else if b = *0 then changes* (*xs* @ [*a*]) *else changes* (*xs* @ [*b*]))
⟨*proof*⟩

lemma *changes-rev*: **fixes** *xs*:: '*a*::*linordered-idom list*
shows *changes* (*rev xs*) = *changes xs*
⟨*proof*⟩

lemma *changes-rev-about*: **fixes** *xs*:: '*a*::*linordered-idom list*
shows *changes* (*replicate* (*p* − *length xs*) *0* @ *rev xs*) = *changes xs*
⟨*proof*⟩

lemma *changes-add-between*:
assumes $a \leq x$ **and** $x \leq b$
shows *changes* (*as* @ [*a*, *b*] @ *bs*) = *changes* (*as* @ [*a*, *x*, *b*] @ *bs*)
⟨*proof*⟩

lemma *changes-all-nonneg*: **assumes** $\bigwedge i$. *nth-default 0 xs i* ≥ 0 **shows** *changes xs* = *0*
⟨*proof*⟩

lemma *changes-pCons*: *changes* (*coeffs* (*pCons 0 f*)) = *changes* (*coeffs f*)
⟨*proof*⟩

lemma *changes-increasing*:
assumes $\bigwedge i$. *i* < *length xs* − *1* ⟹ *xs* ! (*i* + *1*) ≥ *xs* ! *i*
and *length xs* > *1*
and *hd xs* < *0*
and *last xs* > *0*
shows *changes xs* = *1*
⟨*proof*⟩

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* :: *nat* ⇒ *nat* ⇒ *real poly* **where**
Bernstein-Poly-01 j p = (*monom* (*p choose j*) *j*)
∗ (*monom 1* (*p*−*j*) $\circ_p$ [:*1*, −*1*:])

lemma *degree-Bernstein*:
assumes *hb*: $j \leq p$
shows *degree* (*Bernstein-Poly-01 j p*) = *p*
⟨*proof*⟩

lemma *coeff-gt*:
assumes *hb*: $j > p$
shows *Bernstein-Poly-01 j p* = *0*
⟨*proof*⟩

lemma *degree-Bernstein-le*: *degree* (*Bernstein-Poly-01 j p*) ≤ *p*
⟨*proof*⟩

lemma *poly-Bernstein-nonneg*:
assumes $x \geq 0$ **and** $1 \geq x$
shows *poly* (*Bernstein-Poly-01 j p*) $x \geq 0$
⟨*proof*⟩

lemma *Bernstein-symmetry*:
assumes $j \leq p$
shows (*Bernstein-Poly-01 j p*) $\circ_p$ [:*1*, −*1*:] = *Bernstein-Poly-01* (*p*−*j*) *p*
⟨*proof*⟩

2.2 *Bernstein-Poly-01* and *reciprocal-poly*

lemma *Bernstein-reciprocal*:
reciprocal-poly p (*Bernstein-Poly-01 i p*)
= *smult* (*p choose i*) ([:−*1*, *1*:] ^ (*p*−*i*))
⟨*proof*⟩

lemma *Bernstein-reciprocal-translate*:

reciprocal-poly p (*Bernstein-Poly-01 i p*) $\circ_p$ [:*1*, *1*:] =
monom (*p choose i*) (*p* − *i*)
⟨*proof*⟩

lemma *coeff-Bernstein-sum-01*: **fixes** *b*::*nat* ⇒ *real* **assumes** *hi*: *p* ≥ *i*
shows
coeff (*reciprocal-poly p*
($\sum$ *x* = *0*..*p*. *smult* (*b x*) (*Bernstein-Poly-01 x p*)) $\circ_p$ [:*1*, *1*:])
(*p* − *i*) = (*p choose i*) ∗ (*b i*) (**is** *?L* = *?R*)
⟨*proof*⟩

lemma *Bernstein-sum-01*: **assumes** *hP*: *degree P* ≤ *p*
shows
P = ($\sum$ *j* = *0*..*p*. *smult*
(*inverse* (*real* (*p choose j*)) ∗
coeff (*reciprocal-poly p P* $\circ_p$ [:*1*, *1*:]) (*p*−*j*))
(*Bernstein-Poly-01 j p*))
⟨*proof*⟩

lemma *Bernstein-Poly-01-span1*:
assumes *hP*: *degree P* ≤ *p*
shows *P* ∈ *poly-vs.span* {*Bernstein-Poly-01 x p* | *x*. *x* ≤ *p*}
⟨*proof*⟩

lemma *Bernstein-Poly-01-span*:
poly-vs.span {*Bernstein-Poly-01 x p* | *x*. *x* ≤ *p*}
= {*x*. *degree x* ≤ *p*}
⟨*proof*⟩

2.3 Bernstein coefficients and changes

definition *Bernstein-coeffs-01* :: *nat* ⇒ *real poly* ⇒ *real list* **where**
Bernstein-coeffs-01 p P =
[(*inverse* (*real* (*p choose j*)) ∗
coeff (*reciprocal-poly p P* $\circ_p$ [:*1*, *1*:]) (*p*−*j*)). *j* ← [*0*..<(*p*+*1*)]]

lemma *length-Bernstein-coeffs-01*: *length* (*Bernstein-coeffs-01 p P*) = *p* + *1*
⟨*proof*⟩

lemma *nth-default-Bernstein-coeffs-01*: **assumes** *degree P* ≤ *p*
shows *nth-default 0* (*Bernstein-coeffs-01 p P*) *i* =
inverse (*p choose i*) ∗ *coeff* (*reciprocal-poly p P* $\circ_p$ [:*1*, *1*:]) (*p*−*i*)
⟨*proof*⟩

lemma *Bernstein-coeffs-01-sum*: **assumes** *degree P* ≤ *p*
shows *P* = ($\sum$ *j* = *0*..*p*. *smult* (*nth-default 0* (*Bernstein-coeffs-01 p P*) *j*)
(*Bernstein-Poly-01 j p*))
⟨*proof*⟩

definition *Bernstein-changes-01* :: *nat* ⇒ *real poly* ⇒ *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* ← [*0*..<*p* + *1*]])
⟨*proof*⟩

lemma *Bernstein-changes-01-eq-changes*:
assumes *hP*: *degree P* ≤ *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* ≤ *p* **and** *h0*: *P* ≠ *0*
shows *proots-count P* {*x*. *0* < *x* ∧ *x* < *1*} ≤ *Bernstein-changes-01 p P* ∧
even (*Bernstein-changes-01 p P* − *proots-count P* {*x*. *0* < *x* ∧ *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* ≠ *0*
shows *Bernstein-coeffs-01 p* (*monom 1 1*) = [*i*/*p*. *i* ← [*0*..<(*p*+*1*)]]
⟨*proof*⟩

lemma *Bernstein-coeffs-01-add*:
assumes *degree P* ≤ *p* **and** *degree Q* ≤ *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* ≤ *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**
  $Bernstein\text{-}Poly\ j\ p\ c\ d = smult\ ((p\ choose\ j)/(d - c)\hat{\ }p)$
    $(((monom\ 1\ j) \circ_p [:-c,\ 1:]) * (monom\ 1\ (p-j) \circ_p [:d,\ -1:]))$

lemma *Bernstein-Poly-altdef*:
  assumes $c \neq d$ **and** $j \leq p$
  shows $Bernstein\text{-}Poly\ j\ p\ c\ d = smult\ (p\ choose\ j)$
      $([:-c/(d-c),\ 1/(d-c):]\hat{\ }j * [:d/(d-c),\ -1/(d-c):]\hat{\ }(p-j))$
   (**is** $?L = ?R$)
⟨*proof*⟩

lemma *Bernstein-Poly-nonneg*:
  assumes $c \leq x$ **and** $x \leq d$
  shows $poly\ (Bernstein\text{-}Poly\ j\ p\ c\ d)\ x \geq 0$
  ⟨*proof*⟩

lemma *Bernstein-Poly-01*: $Bernstein\text{-}Poly\ j\ p\ 0\ 1 = Bernstein\text{-}Poly\text{-}01\ j\ p$
  ⟨*proof*⟩

lemma *Bernstein-Poly-rescale*:
  assumes $a \neq b$
  shows $Bernstein\text{-}Poly\ j\ p\ c\ d \circ_p [:a,\ 1:] \circ_p [:0,\ b-a:]$
      $= Bernstein\text{-}Poly\ j\ p\ ((c-a)/(b-a))\ ((d-a)/(b-a))$
  (**is** $?L = ?R$)
⟨*proof*⟩

lemma *Bernstein-Poly-rescale-01*:
  assumes $c \neq d$
  shows $Bernstein\text{-}Poly\ j\ p\ c\ d \circ_p [:c,\ 1:] \circ_p [:0,\ d-c:]$
     $= Bernstein\text{-}Poly\text{-}01\ j\ p$
  ⟨*proof*⟩

lemma *Bernstein-Poly-eq-rescale-01*:
  assumes $c \neq d$
  shows $Bernstein\text{-}Poly\ j\ p\ c\ d = Bernstein\text{-}Poly\text{-}01\ j\ p$
      $\circ_p [:0,\ 1/(d-c):] \circ_p [:-c,\ 1:]$
  ⟨*proof*⟩

lemma *coeff-Bernstein-sum*:
  fixes $b{::}nat \Rightarrow real$ **and** $p{::}nat$ **and** $c\ d{::}real$

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

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

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

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

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

3.2 Bernstein coefficients and changes over any interval

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

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

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

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

$(Bernstein\text{-}Poly\ j\ p\ c\ d))$
⟨proof⟩

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

lemma *Bernstein-changes-eq-rescale*: **assumes** $c \neq d$ **and** $degree\ P \leq p$
shows $Bernstein\text{-}changes\ p\ c\ d\ P =$
$Bernstein\text{-}changes\text{-}01\ p\ (P \circ_p [:c,\ 1:] \circ_p [:0,\ d-c:])$
⟨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 $proots\text{-}count\ P\ \{x.\ c < x \wedge x < d\} \leq Bernstein\text{-}changes\ p\ c\ d\ P \wedge$
$even\ (Bernstein\text{-}changes\ p\ c\ d\ P - proots\text{-}count\ P\ \{x.\ c < x \wedge x < d\})$
⟨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
$control\text{-}points\ p\ c\ d\ P =$
$[(((real\ i)*d + (real\ (p - i))*c)/p,$
$nth\text{-}default\ 0\ (Bernstein\text{-}coeffs\ p\ c\ d\ P)\ i).$
$i \leftarrow [0..<(p+1)]]$

lemma *line-above*:
fixes $a\ b\ c\ d$ :: *real* **and** p :: *nat* **and** P :: *real poly*
assumes *hline*: $\bigwedge i.\ i \leq p \Longrightarrow a * (((real\ i)*d + (real\ (p - i))*c)/p) + b \geq$
$nth\text{-}default\ 0\ (Bernstein\text{-}coeffs\ p\ c\ d\ P)\ i$
and *hp*: $p \neq 0$ **and** *hcd*: $c \neq d$ **and** *hP*: $degree\ P \leq p$
shows $\bigwedge x.\ c \leq x \Longrightarrow x \leq d \Longrightarrow a*x + b \geq poly\ P\ x$
⟨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* ⇒ *bool* **where**
normal-poly p ≡
  ($p \neq 0$) ∧
  (∀ i. $0 \leq$ *coeff p i*) ∧
  (∀ i. *coeff p i* ∗ *coeff p* (i+2) ≤ (*coeff p* (i+1))^2) ∧
  (∀ i j k. $i \leq j \longrightarrow j \leq k \longrightarrow 0 <$ *coeff p i*
    ⟶ $0 <$ *coeff p k* ⟶ $0 <$ *coeff p j*)

lemma *normal-non-zero*: *normal-poly p* ⟹ $p \neq 0$
  ⟨*proof*⟩

lemma *normal-coeff-nonneg*: *normal-poly p* ⟹ $0 \leq$ *coeff p i*
  ⟨*proof*⟩

lemma *normal-poly-coeff-mult*:
  normal-poly p ⟹ *coeff p i* ∗ *coeff p* (i+2) ≤ (*coeff p* (i+1))^2
  ⟨*proof*⟩

lemma *normal-poly-pos-interval*:
  normal-poly p ⟹ $i \leq j$ ⟹ $j \leq k$ ⟹ $0 <$ *coeff p i* ⟹ $0 <$ *coeff p k*
    ⟹ $0 <$ *coeff p j*
  ⟨*proof*⟩

lemma *normal-polyI*:
  assumes ($p \neq 0$)
    and (⋀ i. $0 \leq$ *coeff p i*)
    and (⋀ i. *coeff p i* ∗ *coeff p* (i+2) ≤ (*coeff p* (i+1))^2)
    and (⋀ i j k. $i \leq j$ ⟹ $j \leq k$ ⟹ $0 <$ *coeff p i* ⟹ $0 <$ *coeff p k* ⟹ $0 <$
coeff p j)
  shows *normal-poly p*
  ⟨*proof*⟩

lemma *linear-normal-iff*:
  fixes *x*::*real*
  shows *normal-poly* [:$-x$, 1:] ⟷ $x \leq 0$
⟨*proof*⟩

lemma *quadratic-normal-iff*:
  fixes *z*::*complex*
  shows *normal-poly* [:(*cmod z*)^2, -2∗*Re z*, 1:]
    ⟷ *Re z* ≤ 0 ∧ 4∗(*Re z*)^2 ≥ (*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 $0 <$ *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* ≤ *j*
  shows *coeff f* (*h*+*1*) ∗ *coeff f* (*j*+*1*) ≥ *coeff f h* ∗ *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* ≡ *degree f* **and** *dg* ≡ *degree g*
  shows *normal-poly* (*f*∗*g*)
⟨*proof*⟩

lemma *normal-poly-of-roots*:
  fixes *p*::*real poly*
  assumes ⋀*z*. *poly* (*map-poly complex-of-real p*) *z* = *0*
        ⟹ *Re z* ≤ *0* ∧ *4*∗(*Re z*)^*2* ≥ (*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* ≡ *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 fomalised 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 $\bigwedge x$::*complex*. *poly* (*map-poly of-real p*) *x* = *0* $\Longrightarrow$ *Re x* $\leq$ *0*
    and *lead-coeff p* = *1*
  shows *coeff p i* $\geq$ *0*
  ⟨*proof*⟩

definition *circle-01-diam* :: *complex set* **where**
circle-01-diam =
 {*x*. *cmod* (*x* − (*of-nat 1* :: *complex*)/(*of-nat 2*)) < (*real 1*)/(*real 2*)}

lemma *pos-real-map*:
  {*x*::*complex*. *1* / *x* ∈ (λ*x*. *x* + *1*) ' {*x*. *0* < *Re x*}} = *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* ⇒ *real* ⇒ *complex set* **where**
circle-diam l r = {*x*. *cmod* ((*x* − *l*) − (*r* − *l*)/*2*) < (*r* − *l*)/*2*}

lemma *circle-diam-rescale*: **assumes** *l* < *r*
  shows *circle-diam l r* = (λ *x* . (*x*∗(*r* − *l*) + *l*)) ' *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 *degree* $P \leq p$
shows *Bernstein-changes* $p\ l\ r\ P = 0$
⟨*proof*⟩

5.2 One sign change case

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

lemma *upper-circle-map*:
{*x*::*complex. 1* / *x* ∈ (λ*x. x* + *1*) ‘ {*x. Im x* < *sqrt 3* ∗ *Re x*}} = *upper-circle-01*
⟨*proof*⟩

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

lemma *cnj-upper-circle-01*: *cnj* ‘ *upper-circle-01* = *lower-circle-01*
⟨*proof*⟩

lemma *lower-circle-map*:
{*x*::*complex. 1* / *x* ∈ (λ*x. x* + *1*) ‘ {*x. Im x* > − *sqrt 3* ∗ *Re x*}} = *lower-circle-01*
⟨*proof*⟩

lemma *two-circles-01*:
fixes *P*::*real poly*
assumes *hP*: *degree P* ≤ *p* **and** *hP0*: *P* ≠ *0* **and** *hp0*: *p* ≠ *0*
and *h*: *proots-count* (*map-poly of-real P*)
(*upper-circle-01* ∪ *lower-circle-01*) = *1*
shows *Bernstein-changes-01 p P* = *1*
⟨*proof*⟩

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

lemma *upper-circle-rescale*: **assumes** *l* < *r*
shows *upper-circle l r* = (λ *x* . (*x*∗(*r* − *l*) + *l*)) ‘ *upper-circle-01*
⟨*proof*⟩

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

lemma *lower-circle-rescale*:
assumes *l* < *r*
shows *lower-circle l r* = (λ *x* . (*x*∗(*r* − *l*) + *l*)) ‘ *lower-circle-01*

$\langle proof \rangle$

lemma *two-circles*:
  fixes P::*real poly* **and** l r::*real*
  assumes *hlr*: $l < r$
  and *hP*: *degree* $P \leq p$
  and *hP0*: $P \neq 0$
  and *hp0*: $p \neq 0$
  and *h*: *proots-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 *hP*: *degree* $P \leq p$
  and *hP0*: $P \neq 0$
  and *hp0*: $p \neq 0$
shows *proots-count* (*map-poly of-real* P) (*circle-diam* l r) = 0 $\Longrightarrow$
    Bernstein-changes p l r $P = 0$
  and *proots-count* (*map-poly of-real* P)
    (*upper-circle* l r $\cup$ *lower-circle* l r) = 1 $\Longrightarrow$
    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.