Interpolation Polynomials (in HOL-Algebra)

Emin Karayel

March 24, 2023

Abstract

A well known result from algebra is that, on any field, there is exactly one polynomial of degree less than n interpolating n points [1, §7].

This entry contains a formalization of the above result, as well as the following generalization in the case of finite fields F: There are $|F|^{m-n}$ polynomials of degree less than $m \geq n$ interpolating the same n points, where $|F|$ denotes the size of the domain of the field. To establish the result the entry also includes a formalization of Lagrange interpolation, which might be of independent interest.

The formalized results are defined on the algebraic structures from HOL-Algebra, which are distinct from the type-class based structures defined in HOL. Note that there is an existing formalization for polynomial interpolation and, in particular, Lagrange interpolation by Thiemann and Yamada [2] on the type-class based structures in HOL.

Contents

1 Bounded Degree Polynomials

This section contains a definition for the set of polynomials with a degree bound and establishes its cardinality.

theory *Bounded-Degree-Polynomials*
 imports *HOL−Algebra.Polynomial-Divisibility*
begin

lemma (**in** *ring*) *coeff-in-carrier*: $p \in carrier\ (poly\text{-}ring\ R) \Longrightarrow coeff\ p\ i \in carrier\ R$

$\langle proof \rangle$

definition *bounded-degree-polynomials*
where $bounded\text{-}degree\text{-}polynomials\ F\ n = \{x.\ x \in carrier\ (poly\text{-}ring\ F) \wedge (degree\ x < n \vee x = [])\}$

Note: The definition for *bounded-degree-polynomials* includes the zero polynomial in *bounded-degree-polynomials F 0*. The reason for this adjustment is that, contrary to definition in HOL Algebra, most authors set the degree of the zero polynomial to $-\infty$ [1, §7.2.2]. That definition make some identities, such as $\deg(fg) = \deg f + \deg g$ for polynomials f and g unconditionally true. In particular, it prevents an unnecessary corner case in the statement of the results established in this entry.

lemma *bounded-degree-polynomials-length*:
$bounded\text{-}degree\text{-}polynomials\ F\ n = \{x.\ x \in carrier\ (poly\text{-}ring\ F) \wedge length\ x \leq n\}$
$\langle proof \rangle$

lemma (**in** *ring*) *fin-degree-bounded*:
assumes $finite\ (carrier\ R)$
shows $finite\ (bounded\text{-}degree\text{-}polynomials\ R\ n)$
$\langle proof \rangle$

lemma (**in** *ring*) *non-empty-bounded-degree-polynomials*:
$bounded\text{-}degree\text{-}polynomials\ R\ k \neq \{\}$
$\langle proof \rangle$

lemma *in-image-by-witness*:
assumes $\bigwedge x.\ x \in A \Longrightarrow g\ x \in B \wedge f\ (g\ x) = x$
shows $A \subseteq f\ `\ B$
$\langle proof \rangle$

lemma *card-mostly-constant-maps*:
assumes $y \in B$
shows $card\ \{f.\ range\ f \subseteq B \wedge (\forall x.\ x \geq n \longrightarrow f\ x = y)\} = card\ B\ \widehat{}\ n$ (**is** $card\ ?A = ?B$)
$\langle proof \rangle$

definition (**in** *ring*) *build-poly* **where**
$build\text{-}poly\ f\ n = normalize\ (rev\ (map\ f\ [0..{<}n]))$

lemma (**in** *ring*) *poly-degree-bound-from-coeff*:
assumes $x \in carrier\ (poly\text{-}ring\ R)$
assumes $\bigwedge k.\ k \geq n \Longrightarrow coeff\ x\ k = \mathbf{0}$
shows $degree\ x < n \vee x = \mathbf{0}_{poly\text{-}ring\ R}$
$\langle proof \rangle$

lemma (**in** *ring*) *poly-degree-bound-from-coeff-1*:
assumes $x \in carrier\ (poly\text{-}ring\ R)$

assumes $\bigwedge k.\ k \geq n \Longrightarrow$ *coeff x k* $= \mathbf{0}$
shows $x \in$ *bounded-degree-polynomials R n*
⟨*proof*⟩

lemma (**in** *ring*) *length-build-poly*:
length (*build-poly f n*) $\leq n$
⟨*proof*⟩

lemma (**in** *ring*) *build-poly-degree*:
degree (*build-poly f n*) $\leq n-1$
⟨*proof*⟩

lemma (**in** *ring*) *build-poly-poly*:
assumes $\bigwedge i.\ i < n \Longrightarrow f\ i \in$ *carrier R*
shows *build-poly f n* $\in$ *carrier* (*poly-ring R*)
⟨*proof*⟩

lemma (**in** *ring*) *build-poly-coeff*:
coeff (*build-poly f n*) $i =$ (*if* $i < n$ *then* $f\ i$ *else* $\mathbf{0}$)
⟨*proof*⟩

lemma (**in** *ring*) *build-poly-bounded*:
assumes $\bigwedge k.\ k < n \Longrightarrow f\ k \in$ *carrier R*
shows *build-poly f n* $\in$ *bounded-degree-polynomials R n*
⟨*proof*⟩

The following establishes the total number of polynomials with a degree less than n. Unlike the results in the following sections, it is already possible to establish this property for polynomials with coefficients in a ring.

lemma (**in** *ring*) *bounded-degree-polynomials-card*:
card (*bounded-degree-polynomials R n*) = *card* (*carrier R*) ^ *n*
⟨*proof*⟩

end

2 Lagrange Interpolation

This section introduces the function *interpolate*, which constructs the Lagrange interpolation polynomials for a given set of points, followed by a theorem of its correctness.

theory *Lagrange-Interpolation*
imports *HOL−Algebra.Polynomial-Divisibility*
begin

A finite product in a domain is 0 if and only if at least one factor is. This could be added to *HOL−Algebra.FiniteProduct* or *HOL−Algebra.Ring*.

lemma (**in** *domain*) *finprod-zero-iff*:

assumes *finite A*
assumes $\bigwedge a.\ a \in A \Longrightarrow f\ a \in carrier\ R$
shows $finprod\ R\ f\ A = \mathbf{0} \longleftrightarrow (\exists\, x \in A.\ f\ x = \mathbf{0})$
⟨*proof*⟩

lemma (**in** *ring*) *poly-of-const-in-carrier*:
assumes $s \in carrier\ R$
shows $poly\text{-}of\text{-}const\ s \in carrier\ (poly\text{-}ring\ R)$
⟨*proof*⟩

lemma (**in** *ring*) *eval-poly-of-const*:
assumes $x \in carrier\ R$
shows $eval\ (poly\text{-}of\text{-}const\ x)\ y = x$
⟨*proof*⟩

lemma (**in** *ring*) *eval-in-carrier-2*:
assumes $x \in carrier\ (poly\text{-}ring\ R)$
assumes $y \in carrier\ R$
shows $eval\ x\ y \in carrier\ R$
⟨*proof*⟩

lemma (**in** *domain*) *poly-mult-degree-le-1*:
assumes $x \in carrier\ (poly\text{-}ring\ R)$
assumes $y \in carrier\ (poly\text{-}ring\ R)$
shows $degree\ (x \otimes_{poly\text{-}ring\ R}\ y) \le degree\ x + degree\ y$
⟨*proof*⟩

lemma (**in** *domain*) *poly-mult-degree-le*:
assumes $x \in carrier\ (poly\text{-}ring\ R)$
assumes $y \in carrier\ (poly\text{-}ring\ R)$
assumes $degree\ x \le n$
assumes $degree\ y \le m$
shows $degree\ (x \otimes_{poly\text{-}ring\ R}\ y) \le n + m$
⟨*proof*⟩

lemma (**in** *domain*) *poly-add-degree-le*:
assumes $x \in carrier\ (poly\text{-}ring\ R)\ degree\ x \le n$
assumes $y \in carrier\ (poly\text{-}ring\ R)\ degree\ y \le n$
shows $degree\ (x \oplus_{poly\text{-}ring\ R}\ y) \le n$
⟨*proof*⟩

lemma (**in** *domain*) *poly-sub-degree-le*:
assumes $x \in carrier\ (poly\text{-}ring\ R)\ degree\ x \le n$
assumes $y \in carrier\ (poly\text{-}ring\ R)\ degree\ y \le n$
shows $degree\ (x \ominus_{poly\text{-}ring\ R}\ y) \le n$
⟨*proof*⟩

lemma (**in** *domain*) *poly-sum-degree-le*:
assumes *finite A*

assumes $\bigwedge x.\ x \in A \Longrightarrow$ *degree* $(f\ x) \leq n$
assumes $\bigwedge x.\ x \in A \Longrightarrow f\ x \in$ *carrier* (*poly-ring* R)
shows *degree* (*finsum* (*poly-ring* R) $f\ A$) $\leq n$
⟨*proof*⟩

definition (**in** *ring*) *lagrange-basis-polynomial-aux* **where**
lagrange-basis-polynomial-aux S =
($\bigotimes_{poly\text{-}ring\ R}\ s \in S.\ X \ominus_{poly\text{-}ring\ R}$ (*poly-of-const* s))

lemma (**in** *domain*) *lagrange-aux-eval*:
assumes *finite* S
assumes $S \subseteq$ *carrier* R
assumes $x \in$ *carrier* R
shows (*eval* (*lagrange-basis-polynomial-aux* S) x) = ($\bigotimes s \in S.\ x \ominus s$)
⟨*proof*⟩

lemma (**in** *domain*) *lagrange-aux-poly*:
assumes *finite* S
assumes $S \subseteq$ *carrier* R
shows *lagrange-basis-polynomial-aux* $S \in$ *carrier* (*poly-ring* R)
⟨*proof*⟩

lemma (**in** *domain*) *poly-prod-degree-le*:
assumes *finite* A
assumes $\bigwedge x.\ x \in A \Longrightarrow f\ x \in$ *carrier* (*poly-ring* R)
shows *degree* (*finprod* (*poly-ring* R) $f\ A$) $\leq$ ($\sum x \in A.$ *degree* $(f\ x)$)
⟨*proof*⟩

lemma (**in** *domain*) *lagrange-aux-degree*:
assumes *finite* S
assumes $S \subseteq$ *carrier* R
shows *degree* (*lagrange-basis-polynomial-aux* S) $\leq$ *card* S
⟨*proof*⟩

definition (**in** *ring*) *lagrange-basis-polynomial* **where**
lagrange-basis-polynomial $S\ x$ = *lagrange-basis-polynomial-aux* S
$\otimes_{poly\text{-}ring\ R}$ (*poly-of-const* (inv_R ($\bigotimes s \in S.\ x \ominus s$)))

lemma (**in** *field*)
assumes *finite* S
assumes $S \subseteq$ *carrier* R
assumes $x \in$ *carrier* $R - S$
shows
lagrange-one: *eval* (*lagrange-basis-polynomial* $S\ x$) x = **1** **and**
lagrange-degree: *degree* (*lagrange-basis-polynomial* $S\ x$) $\leq$ *card* S **and**
lagrange-zero: $\bigwedge s.\ s \in S \Longrightarrow$ *eval* (*lagrange-basis-polynomial* $S\ x$) s = **0** **and**
lagrange-poly: *lagrange-basis-polynomial* $S\ x \in$ *carrier* (*poly-ring* R)
⟨*proof*⟩

definition (**in** *ring*) *interpolate* **where**
interpolate S f =
$(\bigoplus_{\mathit{poly\text{-}ring}\ R} s \in S.\ \mathit{lagrange\text{-}basis\text{-}polynomial}\ (S - \{s\})\ s \otimes_{\mathit{poly\text{-}ring}\ R} (\mathit{poly\text{-}of\text{-}const}\ (f\ s)))$

Let f be a function and S be a finite subset of the domain of the field. Then *interpolate S f* will return a polynomial with degree less than *card S* interpolating f on S.

theorem (**in** *field*)
assumes *finite S*
assumes $S \subseteq \mathit{carrier}\ R$
assumes $f\ `\ S \subseteq \mathit{carrier}\ R$
shows
interpolate-poly: $\mathit{interpolate}\ S\ f \in \mathit{carrier}\ (\mathit{poly\text{-}ring}\ R)$ **and**
interpolate-degree: $\mathit{degree}\ (\mathit{interpolate}\ S\ f) \leq \mathit{card}\ S - 1$ **and**
interpolate-eval: $\bigwedge s.\ s \in S \Longrightarrow \mathit{eval}\ (\mathit{interpolate}\ S\ f)\ s = f\ s$
⟨*proof*⟩

end

3 Cardinalities of Interpolation Polynomials

This section establishes the cardinalities of the set of polynomials with a degree bound interpolating a given set of points.

theory *Interpolation-Polynomial-Cardinalities*
imports *Bounded-Degree-Polynomials Lagrange-Interpolation*
begin

lemma (**in** *ring*) *poly-add-coeff*:
assumes $x \in \mathit{carrier}\ (\mathit{poly\text{-}ring}\ R)$
assumes $y \in \mathit{carrier}\ (\mathit{poly\text{-}ring}\ R)$
shows $\mathit{coeff}\ (x \oplus_{\mathit{poly\text{-}ring}\ R} y)\ k = \mathit{coeff}\ x\ k \oplus \mathit{coeff}\ y\ k$
⟨*proof*⟩

lemma (**in** *domain*) *poly-neg-coeff*:
assumes $x \in \mathit{carrier}\ (\mathit{poly\text{-}ring}\ R)$
shows $\mathit{coeff}\ (\ominus_{\mathit{poly\text{-}ring}\ R}\ x)\ k = \ominus \mathit{coeff}\ x\ k$
⟨*proof*⟩

lemma (**in** *domain*) *poly-substract-coeff*:
assumes $x \in \mathit{carrier}\ (\mathit{poly\text{-}ring}\ R)$
assumes $y \in \mathit{carrier}\ (\mathit{poly\text{-}ring}\ R)$
shows $\mathit{coeff}\ (x \ominus_{\mathit{poly\text{-}ring}\ R} y)\ k = \mathit{coeff}\ x\ k \ominus \mathit{coeff}\ y\ k$
⟨*proof*⟩

A polynomial with more zeros than its degree is the zero polynomial.

lemma (**in** *field*) *max-roots*:

assumes $p \in$ *carrier* (*poly-ring* R)
assumes $K \subseteq$ *carrier* R
assumes *finite* K
assumes *degree* $p <$ *card* K
assumes $\bigwedge x.\ x \in K \Longrightarrow$ *eval* $p\ x = \mathbf{0}$
shows $p = \mathbf{0}_{poly\text{-}ring\ R}$
⟨*proof*⟩

definition (**in** *ring*) *split-poly*
where *split-poly* $K\ p = ($*restrict* (*eval* p) K, $\lambda k.$ *coeff* $p\ (k+$*card* $K))$

To establish the count of the number of polynomials of degree less than n interpolating a function f on K where $|K| \leq n$, the function *split-poly* K establishes a bijection between the polynomials of degree less than n and the values of the polynomials on K in combination with the coefficients of order $|K|$ and greater.

For the injectivity: Note that the difference of two polynomials whose coefficients of order $|K|$ and larger agree must have a degree less than $|K|$ and because their values agree on k points, it must have $|K|$ zeros and hence is the zero polynomial.

For the surjectivty: Let p be a polynomial whose coefficients larger than $|K|$ are chosen, and all other coefficients be 0. Now it is possible to find a polynomial q interpolating $f - p$ on K using Lagrange interpolation. Then $p + q$ will interpolate f on K and because the degree of q is less than $|K|$ its coefficients of order $|K|$ will be the same as those of p.

A tempting question is whether it would be easier to instead establish a bijection between the polynomials of degree less than n and its values on $K \cup K'$ where K' are arbitrarily chosen $n - |K|$ points in the field. This approach is indeed easier, however, it fails for the case where the size of the field is less than n.

lemma (**in** *field*) *split-poly-inj*:
assumes *finite* K
assumes $K \subseteq$ *carrier* R
shows *inj-on* (*split-poly* K) (*carrier* (*poly-ring* R))
⟨*proof*⟩

lemma (**in** *field*) *split-poly-image*:
assumes *finite* K
assumes $K \subseteq$ *carrier* R
shows *split-poly* K ‘ *carrier* (*poly-ring* R) $\supseteq$
$(K \rightarrow_E$ *carrier* $R) \times \{f.$ *range* $f \subseteq$ *carrier* $R \wedge (\exists\, n.\ \forall\, k \geq n.\ f\ k = \mathbf{0}_R)\}$
⟨*proof*⟩

This is like *card-vimage-inj* but supports *inj-on* instead.

lemma *card-vimage-inj-on*:
assumes *inj-on* $f\ B$

assumes $A \subseteq f \text{ ` } B$
shows $\mathit{card}\ (f -\text{` } A \cap B) = \mathit{card}\ A$
$\langle \mathit{proof} \rangle$

lemma *inv-subsetI*:
assumes $\bigwedge x.\ x \in A \Longrightarrow f\ x \in B \Longrightarrow x \in C$
shows $f -\text{` } B \cap A \subseteq C$
$\langle \mathit{proof} \rangle$

The following establishes the main result of this section: There are $|F|^{n-k}$ polynomials of degree less than n interpolating $k \leq n$ points.

lemma *restrict-eq-imp*:
assumes $\mathit{restrict}\ f\ A = \mathit{restrict}\ g\ A$
assumes $x \in A$
shows $f\ x = g\ x$
$\langle \mathit{proof} \rangle$

theorem (**in** *field*) *interpolating-polynomials-card*:
assumes $\mathit{finite}\ K$
assumes $K \subseteq \mathit{carrier}\ R$
assumes $f \text{ ` } K \subseteq \mathit{carrier}\ R$
shows $\mathit{card}\ \{\omega \in \mathit{bounded\text{-}degree\text{-}polynomials}\ R\ (\mathit{card}\ K + n).\ (\forall k \in K.\ \mathit{eval}\ \omega\ k = f\ k)\} = \mathit{card}\ (\mathit{carrier}\ R)\hat{\ }n$
(**is** $\mathit{card}\ ?A = ?B$)
$\langle \mathit{proof} \rangle$

A corollary is the classic result [1, Theorem 7.15] that there is exactly one polynomial of degree less than n interpolating n points:

corollary (**in** *field*) *interpolating-polynomial-one*:
assumes $\mathit{finite}\ K$
assumes $K \subseteq \mathit{carrier}\ R$
assumes $f \text{ ` } K \subseteq \mathit{carrier}\ R$
shows $\mathit{card}\ \{\omega \in \mathit{bounded\text{-}degree\text{-}polynomials}\ R\ (\mathit{card}\ K).\ (\forall k \in K.\ \mathit{eval}\ \omega\ k = f\ k)\} = 1$
$\langle \mathit{proof} \rangle$

In the case of fields with infinite carriers, it is possible to conclude that there are infinitely many polynomials of degree less than n interpolating $k < n$ points.

corollary (**in** *field*) *interpolating-polynomial-inf*:
assumes $\mathit{infinite}\ (\mathit{carrier}\ R)$
assumes $\mathit{finite}\ K\ K \subseteq \mathit{carrier}\ R\ f \text{ ` } K \subseteq \mathit{carrier}\ R$
assumes $n > 0$
shows $\mathit{infinite}\ \{\omega \in \mathit{bounded\text{-}degree\text{-}polynomials}\ R\ (\mathit{card}\ K + n).\ (\forall k \in K.\ \mathit{eval}\ \omega\ k = f\ k)\}$
(**is** $\mathit{infinite}\ ?A$)
$\langle \mathit{proof} \rangle$

The following is an additional independent result: The evaluation homomorphism is injective for degree one polynomials.

lemma (**in** *field*) *eval-inj-if-degree-1*:
  assumes $p \in carrier\ (poly\text{-}ring\ R)\ degree\ p = 1$
  shows *inj-on* (*eval p*) (*carrier R*)
⟨*proof*⟩

end

References

[1] V. Shoup. *A Computational Introduction to Number theory and Algebra.* Cambridge university press, 2009.

[2] R. Thiemann and A. Yamada. Polynomial interpolation. *Archive of Formal Proofs*, Jan. 2016. https://isa-afp.org/entries/Polynomial_Interpolation.html, Formal proof development.