# Interpolation Polynomials (in HOL-Algebra) 

Emin Karayel

March 11, 2024


#### 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 1
2 Lagrange Interpolation 3
3 Cardinalities of Interpolation Polynomials 6

## 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-ring $R) \Longrightarrow$ coeff $p i \in$ carrier R

```
    <proof\rangle
definition bounded-degree-polynomials
    where bounded-degree-polynomials F n ={x. x carrier (poly-ring F) ^(degree
x<n\veex=[])}
```

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 $-\infty[1, \S 7.2 .2]$. That definition make some identities, such as $\operatorname{deg}(f g)=\operatorname{deg} f+\operatorname{deg} g$ 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-degree-polynomials \(F n=\{x . x \in\) carrier \((\) poly-ring \(F) \wedge\) length \(x \leq n\}\)
    \(\langle p r o o f\rangle\)
lemma (in ring) fin-degree-bounded:
    assumes finite (carrier \(R\) )
    shows finite (bounded-degree-polynomials \(R n\) )
\(\langle p r o o f\rangle\)
lemma (in ring) non-empty-bounded-degree-polynomials:
    bounded-degree-polynomials \(R k \neq\{ \}\)
〈proof〉
lemma in-image-by-witness:
    assumes \(\wedge x . x \in A \Longrightarrow g x \in B \wedge f(g x)=x\)
    shows \(A \subseteq f^{\prime} B\)
    \(\langle p r o o f\rangle\)
lemma card-mostly-constant-maps:
    assumes \(y \in B\)
    shows card \(\{f\). range \(f \subseteq B \wedge(\forall x . x \geq n \longrightarrow f x=y)\}=\operatorname{card} B{ }^{\wedge} n\) (is card
\(? A=? B)\)
\(\langle p r o o f\rangle\)
definition (in ring) build-poly where
    build-poly \(f=\) normalize \((\operatorname{rev}(\operatorname{map} f[0 . .<n]))\)
lemma (in ring) poly-degree-bound-from-coeff:
    assumes \(x \in\) carrier (poly-ring \(R\) )
    assumes \(\bigwedge k . k \geq n \Longrightarrow\) coeff \(x k=\mathbf{0}\)
    shows degree \(x<n \vee x=\mathbf{0}_{\text {poly-ring } R}\)
\(\langle p r o o f\rangle\)
```

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

```
assumes }\bigwedgek.k\geqn\Longrightarrow\mathrm{ coeff }xk=\mathbf{0
shows }x\in\mathrm{ bounded-degree-polynomials }R
<proof>
lemma (in ring) length-build-poly:
length (build-poly f n) \leqn
<proof>
lemma (in ring) build-poly-degree:
    degree (build-poly f n) \leqn-1
    <proof\rangle
lemma (in ring) build-poly-poly:
    assumes \bigwedgei. i<n\Longrightarrowfi\in carrier R
    shows build-poly f n c carrier (poly-ring R)
    <proof\rangle
lemma (in ring) build-poly-coeff:
    coeff (build-poly f n) i=(if i<n then fi else 0)
<proof>
lemma (in ring) build-poly-bounded:
    assumes \k. k<n\Longrightarrowfk\in carrier R
    shows build-poly f n \in bounded-degree-polynomials }R
    <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) ^}
<proof\rangle
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 $H O L-$ Algebra.FiniteProduct or HOL-Algebra.Ring.
lemma (in domain) finprod-zero-iff:

```
assumes finite A
assumes \a.a\inA\Longrightarrowfa\in carrier R
shows finprod R f A=0 < \longleftrightarrow(\existsx\inA.fx=0)
\langleproof\rangle
lemma (in ring) poly-of-const-in-carrier:
assumes }s\in\mathrm{ carrier R
shows poly-of-const s\incarrier (poly-ring R)
<proof>
lemma (in ring) eval-poly-of-const:
assumes x carrier R
shows eval (poly-of-const x) y =x
<proof>
lemma (in ring) eval-in-carrier-2:
assumes }x\in\mathrm{ carrier (poly-ring R)
assumes y carrier R
shows eval x y carrier R
<proof\rangle
lemma (in domain) poly-mult-degree-le-1:
assumes }x\in\mathrm{ carrier (poly-ring R)
assumes y carrier (poly-ring R)
shows degree (x \otimes poly-ring R y) \leq degree }x+\mathrm{ degree }
<proof\rangle
lemma (in domain) poly-mult-degree-le:
assumes }x\in\mathrm{ carrier (poly-ring R)
assumes }y\in\mathrm{ carrier (poly-ring R)
assumes degree }x\leq
assumes degree }y\leq
shows degree ( }x\mp@subsup{\otimes}{\mathrm{ poly-ring R}}{}y)\leqn+
<proof>
lemma (in domain) poly-add-degree-le:
assumes }x\in\mathrm{ carrier (poly-ring R) degree }x\leq
assumes }y\in\mathrm{ carrier (poly-ring R) degree }y\leq
shows degree ( }x\mp@subsup{\oplus}{\mathrm{ poly-ring R}}{}y)\leq
<proof\rangle
lemma (in domain) poly-sub-degree-le:
    assumes }x\in\mathrm{ carrier (poly-ring R) degree }x\leq
    assumes }y\in\mathrm{ carrier (poly-ring R) degree }y\leq
    shows degree ( }x\mp@subsup{\ominus}{\mathrm{ poly-ring R }}{
<proof>
lemma (in domain) poly-sum-degree-le: assumes finite \(A\)
```

```
assumes }\x.x\inA\Longrightarrow\mathrm{ degree ( }fx)\leq
assumes }\x.x\inA\Longrightarrowfx\incarrier (poly-ring R
shows degree (finsum (poly-ring R)fA)\leqn
<proof\rangle
definition (in ring) lagrange-basis-polynomial-aux where
    lagrange-basis-polynomial-aux S=
    (}\mp@subsup{\otimes}{\mathrm{ poly-ring R}}{
lemma (in domain) lagrange-aux-eval:
    assumes finite S
    assumes S\subseteqcarrier R
    assumes x \in carrier R
    shows (eval (lagrange-basis-polynomial-aux S) x) =(囚s\inS.x\ominuss)
<proof>
lemma (in domain) lagrange-aux-poly:
    assumes finite S
    assumes S\subseteqcarrier R
    shows lagrange-basis-polynomial-aux S carrier (poly-ring R)
<proof\rangle
lemma (in domain) poly-prod-degree-le:
    assumes finite }
    assumes }\x.x\inA\Longrightarrowfx\incarrier (poly-ring R
    shows degree (finprod (poly-ring R) fA)\leq(\sumx\inA. degree (fx))
    <proof\rangle
lemma (in domain) lagrange-aux-degree:
    assumes finite S
    assumes S\subseteqcarrier R
    shows degree (lagrange-basis-polynomial-aux S)}\leq\operatorname{card}
<proof\rangle
definition (in ring) lagrange-basis-polynomial where
    lagrange-basis-polynomial Sx= lagrange-basis-polynomial-aux S
    \otimes poly-ring R (poly-of-const (inv 
lemma (in field)
    assumes finite S
    assumes S\subseteqcarrier R
    assumes x carrier R-S
    shows
    lagrange-one: eval (lagrange-basis-polynomial S x) x=1 and
    lagrange-degree:degree (lagrange-basis-polynomial S x) \leqcard S and
    lagrange-zero: \s. s\inS\Longrightarrow eval (lagrange-basis-polynomial Sx) s=0 0 and
    lagrange-poly: lagrange-basis-polynomial S x carrier (poly-ring R)
<proof>
```

```
definition (in ring) interpolate where
    interpolate S f=
    ( }\mp@subsup{\bigoplus}{\mathrm{ poly-ring }\mp@subsup{R}{}{s}\inS.lagrange-basis-polynomial (S - {s})s 的oly-ring R (poly-of-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\subseteqcarrier R
    assumes f'S\subseteqcarrier R
    shows
        interpolate-poly: interpolate S f \in carrier (poly-ring R) and
        interpolate-degree: degree (interpolate S f) \leqcard S-1 and
        interpolate-eval: \s. s\inS\Longrightarrow eval (interpolate S f) s=fs
<proof\rangle
```

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 $x \in$ carrier (poly-ring $R$ )
assumes $y \in$ carrier (poly-ring $R$ )
shows coeff $\left(x \oplus_{\text {poly-ring } R} y\right) k=$ coeff $x k \oplus$ coeff $y k$
$\langle p r o o f\rangle$
lemma (in domain) poly-neg-coeff:
assumes $x \in$ carrier (poly-ring $R$ )
shows coeff $\left(\ominus_{\text {poly-ring }} R^{x}\right) k=\ominus$ coeff $x k$
$\langle p r o o f\rangle$
lemma (in domain) poly-substract-coeff:
assumes $x \in$ carrier (poly-ring $R$ )
assumes $y \in$ carrier (poly-ring $R$ )
shows coeff $\left(x \ominus_{\text {poly-ring }} R\right.$ y) $k=$ coeff $x k \ominus$ coeff $y k$
$\langle p r o o f\rangle$
A polynomial with more zeros than its degree is the zero polynomial.
lemma (in field) max-roots:

```
    assumes p}\in\mathrm{ carrier (poly-ring R)
    assumes K\subseteqcarrier R
    assumes finite K
    assumes degree p< card K
    assumes }\x.x\inK\Longrightarrow eval p x=0
    shows p=\mp@subsup{0}{\mathrm{ poly-ring }R}{}
<proof\rangle
definition (in ring) split-poly
    where split-poly K p = (restrict (eval p) K, \lambdak. 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 $K \cup K^{\prime}$ where $K^{\prime}$ 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))
\(\langle p r o o f\rangle\)
lemma (in field) split-poly-image:
    assumes finite \(K\)
    assumes \(K \subseteq\) carrier \(R\)
    shows split-poly \(K\) ' carrier (poly-ring \(R\) ) \(\supseteq\)
        \(\left(K \rightarrow_{E}\right.\) carrier \(\left.R\right) \times\left\{f\right.\). range \(f \subseteq\) carrier \(\left.R \wedge\left(\exists n . \forall k \geq n . f k=\mathbf{0}_{R}\right)\right\}\)
\(\langle p r o o f\rangle\)
```

This is like card-vimage-inj but supports inj-on instead.
lemma card-vimage-inj-on:
assumes inj-on $f B$

```
assumes \(A \subseteq f^{\prime} B\)
shows \(\operatorname{card}\left(f-{ }^{\prime} A \cap B\right)=\operatorname{card} A\)
\(\langle\) proof \(\rangle\)
lemma inv-subsetI:
assumes \(\bigwedge x . x \in A \Longrightarrow f x \in B \Longrightarrow x \in C\)
shows \(f-{ }^{\prime} B \cap A \subseteq C\)
\(\langle p r o o f\rangle\)
```

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 restrict f A = restrict g A
    assumes }x\in
    shows f}x=g
    \langleproof\rangle
```

theorem (in field) interpolating-polynomials-card:
assumes finite $K$
assumes $K \subseteq$ carrier $R$
assumes $f$ ' $K \subseteq$ carrier $R$
shows card $\{\omega \in$ bounded-degree-polynomials $R$ (card $K+n) .(\forall k \in K$. eval $\omega$
$k=f k)\}=\operatorname{card}($ carrier $R){ }^{\wedge} n$
(is card ? $A=? B$ )
$\langle p r o o f\rangle$

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 finite $K$
assumes $K \subseteq$ carrier $R$
assumes $f^{\prime} K \subseteq$ carrier $R$
shows card $\{\omega \in$ bounded-degree-polynomials $R$ (card $K) .(\forall k \in K$. eval $\omega k=$ $f k)\}=1$
$\langle p r o o f\rangle$
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 infinite (carrier \(R\) )
    assumes finite \(K K \subseteq\) carrier \(R f^{\text {' }} K \subseteq\) carrier \(R\)
    assumes \(n>0\)
    shows infinite \(\{\omega \in\) bounded-degree-polynomials \(R\) (card \(K+n) .(\forall k \in K\). eval
\(\omega k=f k)\}\)
    (is infinite ?A)
\(\langle p r o o f\rangle\)
```

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\mathrm{ carrier (poly-ring R) degree p=1
    shows inj-on (eval p) (carrier R)
<proof\rangle
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.

