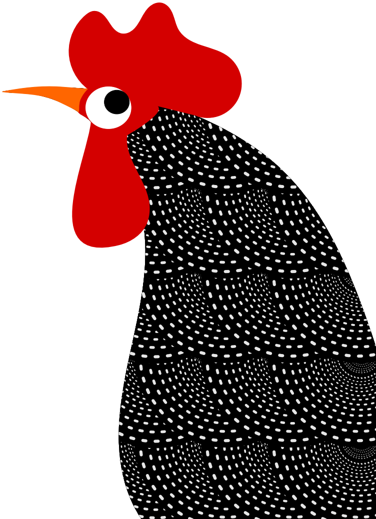
The Polynomials

Laurence Rideau
21 January 2016

COQ WINTER SCHOOL 2016

SOPHIA ANTIPOLIS, FRANCE / 18-22 January



Outline

The Polynomials

Library

A library for univariate polynomials over

- ring structures

with extensions for polynomials whose coefficients range over

- commutative rings
- integral domains

Polynomials

Definitions

$$P = a_n X^n + \ldots + a_2 X^2 + a_1 X + a_0$$

Polynomials
Definitions

$$P = a_n X^n + \ldots + a_2 X^2 + a_1 X + a_0$$

- list of coefficients (decreasing/increasing degrees)
- list of pairs (degree, coef)

Polynomials

Definitions

$$P = a_n X^n + \ldots + a_2 X^2 + a_1 X + a_0$$

- list of coefficients (decreasing/increasing degrees)
- list of pairs (degree, coef)

$$P = a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n$$

A *normalized* (no trailing 0) sequence of coefficients

```
Record polynomial (R : ringType) := Polynomial
  {polyseq :> seq R; _ : last 1 polyseq != 0}.
```

Polynomials

first properties

Polynomials are coercible to sequences:

- one can directly take the k^{th} element of a polynomial (`P`_k`), i.e. retrieve the coefficient of $X^k$ in `P`.
- size of a polynomial
- the degree of a polynomial is its size minus 1

Polynomials

Notations

Notations:

- `{poly R}` - polynomials over `R` (a Ring)
- `Poly s` - the polynomial built from sequence `s`
- `'X` - monomial
- `'X^n` - monomial to the power of `n`
- `a%:P` - constant polynomial
- standard notations of ssralg (`+`, `-`, `*`, `*:`, `^+`)

Polynomials

Notations

Notations:

- `{poly R}` - polynomials over `R` (a Ring)
- `Poly s` - the polynomial built from sequence `s`
- `'X` - monomial
- `'X^n` - monomial to the power of `n`
- `a%:P` - constant polynomial
- standard notations of ssralg (`+`, `-`, `*`, `*:`, `^+`)

A polynomial can be defined by extension:

```
\poly_{i < n} E i
```

is the polynomial:

```
(E 0)+ (E 1) *: 'X
+···+ E (n - 1) *: 'X^(n-1)
```

Polynomials

Ring operations

```
Definition add_poly (p q : {poly R}) :=
\poly_(i < maxn (size p) (size q)) (p`_i + q`_i).
```

Polynomials

Ring operations

```
Definition add_poly (p q : {poly R}) :=
\poly_(i < maxn (size p) (size q)) (p`_i + q`_i).
```

$$\left(\sum_{i=0}^{n} \alpha_i X^i\right)\left(\sum_{i=0}^{m} \beta_i X^i\right) = \sum_{i=0}^{n+m}\left(\sum_{j\leq i} \alpha_j \beta_{i-j}\right) X^i$$

Polynomials

Ring operations

```
Definition add_poly (p q : {poly R}) :=
\poly_(i < maxn (size p) (size q)) (p`_i + q`_i).
```

$$\left(\sum_{i=0}^{n} \alpha_i X^i\right) \left(\sum_{i=0}^{m} \beta_i X^i\right) = \sum_{i=0}^{n+m} \left(\sum_{j \leq i} \alpha_j \beta_{i-j}\right) X^i$$

```
Definition mul_poly (p q : {poly R}) :=
  \poly_(i < (size p + size q).-1)
    (\sum_(j < i.+1) p`_j * q`_(i - j)).
```

Polynomials

Structures

The type of polynomials has been equipped with a (commutative / integral) ring structure.

All related lemmas of `ssralg` can be used.

Polynomials

Evaluation

(Right-)evaluation of polynomials:

```
Fixpoint horner s x :=
  if s is a :: s'
    then horner s' x * x + a
    else 0.
```

```
Notation "p .[ x ]" := (horner p x).
```

Warning: type of x.

Polynomials

Properties of coefficients

```
(* Lifting a ring predicate to polynomials. *)
Definition polyOver (S : pred_class) :=
  [qualify a p : {poly R} | all (mem S) p].
```

```
Lemma polyOver_poly (S : pred_class) n E :
  (forall i, i < n -> E i \in S) -> \poly_(i < n)
      E i \is a polyOver S.
```

NB. predicate associate to S: at least an addrPred

- polyOver0
- polyOverC
- polyOverX
- rpred* (from ssralg)

Derivative

```
Definition deriv p :=
  poly_(i < (size p).-1) (p`_i.+1 *+ i.+1).

Local Notation "p ^` ()" := (deriv p).

Fact deriv_is_linear : linear deriv.

Lemma derivM p q :
(p * q)^`() = p^`() * q + p * q^`().

Definition derivn n p := iter n deriv p.
```

NB. polyOver_deriv

Roots

```
root p x == x is a root of p
   i.e., p.[x] = 0
```

```
Theorem factor_theorem p a :
  reflect (exists q, p = q * ('X - a%:P))
      (root p a).

Theorem max_poly_roots p rs :
  p != 0 -> all (root p) rs -> uniq rs ->
   size rs < size p.
```