Homomorphisms continued

Patrik Jansson

$$\text{-- } h : A \to B \text{ is a homomorphism from } Op : A \to A \to A \text{ to } op : B \to B \to B$$
$$H_2\ (h, Op, op) = \forall\ x.\ \forall\ y.\ h\ (Op\ x\ y) == op\ (h\ x)\ (h\ y)$$
$$\text{-- } h : A \to B \text{ is a homomorphism from } F : A \to A \text{ to } f : B \to B$$
$$H_1\ (h, F, f) \quad = \forall\ x.\ h\ (F\ x) == f\ (h\ x)$$
$$\text{-- } h : A \to B \text{ is a homomorphism from } E : A \text{ to } e : B$$
$$H_0\ (h, E, e) \quad = h\ E == e$$

Homomorphisms continued

Patrik Jansson

$$\text{-- } h : A \to B \text{ is a homomorphism from } Op : A \to A \to A \text{ to } op : B \to B \to B$$
$$H_2\ (h, Op, op) = \forall\ x.\ \forall\ y.\ h\ (Op\ x\ y) == op\ (h\ x)\ (h\ y)$$
$$\text{-- } h : A \to B \text{ is a homomorphism from } F : A \to A \text{ to } f : B \to B$$
$$H_1\ (h, F, f) \quad = \forall\ x.\ h\ (F\ x) == f\ (h\ x)$$
$$\text{-- } h : A \to B \text{ is a homomorphism from } E : A \text{ to } e : B$$
$$H_0\ (h, E, e) \quad = h\ E == e$$

$$MonHom\ (h, (A, Op, E), (B, op, e)) \stackrel{def}{=}$$
$$H_2(h, Op, op) \wedge H_0(h, E, e)$$

"Monoid homomorphism from A to B"

Homomorphisms continued

Patrik Jansson

-- $h : A \to B$ is a homomorphism from $Op : A \to A \to A$ to $op : B \to B \to B$

$H_2\ (h, Op, op) = \forall\ x.\ \forall\ y.\ h\ (Op\ x\ y) == op\ (h\ x)\ (h\ y)$

-- $h : A \to B$ is a homomorphism from $F : A \to A$ to $f : B \to B$

$H_1\ (h, F, f) \quad = \forall\ x.\ h\ (F\ x) == f\ (h\ x)$

-- $h : A \to B$ is a homomorphism from $E : A$ to $e : B$

$H_0\ (h, E, e) \quad = h\ E == e$

$\exists B.\ MonHom\ (h, A, B)$? Is there a monoid structure on B s.t. h is a MonHom?

(B, op, e)

"Monoid homomorphism from A to B"

Homomorphisms continued

Patrik Jansson

$\exists B.\ \mathrm{MonHom}(h, A, B)$? Is there a monoid structure on B s.t. h is a MonHom?

B : (B, op, e)

More generally: $h : Syn \to Sem$

$\mathrm{StructHom}(h, Syn, Sem) \stackrel{def}{=}$

$$\exists c_1, c_2, \ldots c_n.\ \bigwedge_{i=1}^{n} H_{a_i}(h, C_i, c_i)$$

arity $a_i : \mathbb{N}$

where $C_i : Syn \to Syn \to \ldots \to Syn$

$c_i : Sem \to Sem \to \ldots \to Sem$

Homomorphisms continued

Patrik Jansson

$h : Syn \to Sem$

$StructHom\ (h, Syn, Sem) \stackrel{def}{=}$

$$\exists c_1, c_2, \ldots c_n .\ \bigwedge_{i=1}^{n} H_{a_i}(h, C_i, c_i)$$

where $a_i : \mathbb{N}$ is the arity

where $C_i : Syn \to Syn \to \ldots \to Syn$

$c_i : Sem \to Sem \to \ldots \to Sem$

```
data E where
  Add : E → E → E
  Neg : E → E
  Zero : E
```

Example:

```
eval (Add x y) = add (eval x) (eval y)
eval (Neg x)   = neg (eval x)
eval Zero      = zero
```

StructHom (eval, E, Sem) "by definition"

Polynomials

Patrik Jansson

A **polynomial** is a function P whose value at x is

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where a_n, a_{n-1}, …, a_1, and a_0, called the **coefficients** of the polynomial [*sic*], are constants and, if $n > 0$, then $a_n \neq 0$. The number n, the degree of the highest power of x in the polynomial, is called the **degree** of the polynomial. (The degree of the zero polynomial is not defined.)

$P : X \to Y$

$X \subseteq \mathbb{R}$

$Y \subseteq \mathbb{R}$

Types:

$P : \mathbb{R} \to \mathbb{R}$

$x : \mathbb{R}$

$a_n : \mathbb{R}$

$a_0 : \mathbb{R}$

$a : \mathbb{N} \to \mathbb{R}$

$n : \mathbb{N}$

Polynomials

Patrik Jansson

A **polynomial** is a function P whose value at x is

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where a_n, a_{n-1}, ..., a_1, and a_0, called the **coefficients** of the polynomial [*sic*], are constants and, if $n > 0$, then $a_n \neq 0$. The number n, the degree of the highest power of x in the polynomial, is called the **degree** of the polynomial. (The degree of the zero polynomial is not defined.)

Types: $n : \mathbb{N}$

$a : \{0..n\} \to \mathbb{R}$

($x : \mathbb{R}$

$P : \mathbb{R} \to \mathbb{R}$

or $a : [\mathbb{R}]$ (of length $n+1$))

$index : [\mathbb{R}] \to \{0..n\} \to \mathbb{R}$

index as i syntax "a_i"

Polynomials

Patrik Jansson

A **polynomial** is a function P whose value at x is

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where a_n, a_{n-1}, …, a_1, and a_0, called the **coefficients** of the polynomial [*sic*], are constants and, if $n > 0$, then $a_n \neq 0$. The number n, the degree of the highest power of x in the polynomial, is called the **degree** of the polynomial. (The degree of the zero polynomial is not defined.)

Types: $n : \mathbb{N}$

$a : \{0..n\} \to \mathbb{R}$

($x : \mathbb{R}$

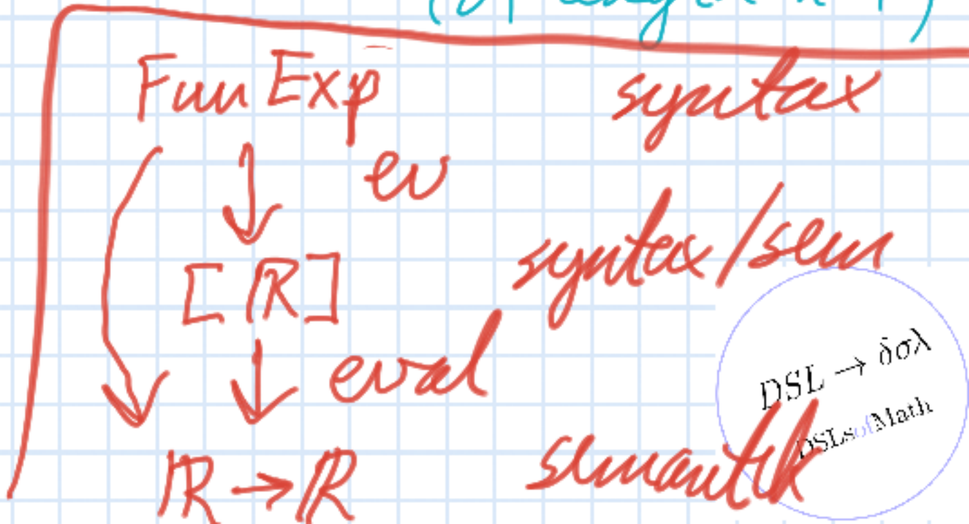
$P : \mathbb{R} \to \mathbb{R}$

or $a : [\mathbb{R}]$ (of length $n+1$))

Syntax: a list of coefficients

Semantics: a "polynomial" function

eval : $[\mathbb{R}] \to (\mathbb{R} \to \mathbb{R})$



Polynomials

Patrik Jansson

Syntax: a list of coefficients

Semantics: a "polynomial" function

$$eval : [\mathbb{R}] \to (\mathbb{R} \to \mathbb{R})$$

```
eval []       x = 0
eval (a : as) x =
  a + x * (eval as x)
```

$$\sum_{i=0}^{n} a_i x^i = a_0 + \sum_{i=1}^{n} a_i \cdot x^i = a_0 + x \cdot \sum_{i=1}^{n} a_i x^{i-1}$$

$$= a_0 + x \cdot \sum_{i=0}^{n-1} a_{i+1} \cdot x^i = a_0 + x \cdot eval\ as\ x$$

Examples

as	eval as
[1, -2, 1]	\x → (x-1)^2
[0, 1]	\x → x
[c]	\x → c
||	
c : []	

DSL → δσλ

DSLsofMath

Polynomials

Patrik Jansson

Syntax: a list of coefficients

Semantics: a "polynomial" function

```
eval : [ℝ] → (ℝ → ℝ)
eval []       x = 0
eval (a : as) x =
  a + x · (eval as x)
```

Examples

as	eval as
[1,-2,1]	\x → (x-1)^2
[0,1]	\x → x
[c]	\x → c

Chebyshev polynomials

Patrik Jansson

Specification: $H, (\cos, (n\cdot), T_n)$ $\quad n : \mathbb{N}$

Claim: T_n is a polynomial function of degree n

Typing: $\cos : \mathbb{R}^+ \to I$ where $I = \{x : \mathbb{R} \mid -1 \leq x \leq 1\}$

$(n\cdot) : \mathbb{R}^+ \to \mathbb{R}^+$

$T_n : I \to I$

Expanded: $\forall v : \mathbb{R}^+.\ \cos(n \cdot v) == T_n(\cos v)$

$n = 0$: $\cos 0 == T_0(\cos v)$ thus $T_0\ x = 1$

$n = 1$: $\cos v == T_1(\cos v)$ thus $T_1\ x = x$

Chebyshev polynomials

Patrik Jansson

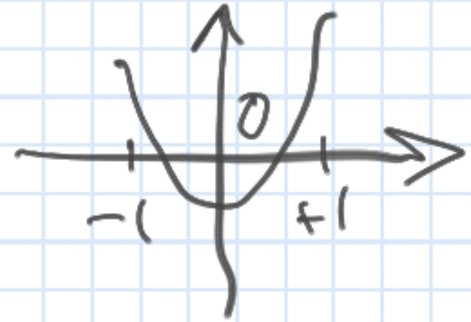
Specification: $H, (\cos, (n\cdot), T_n)$

Claim: T_n is a polynomial function of degree n

Typing: $\cos : \mathbb{R}^+ \to I$ where $I = \{x : \mathbb{R} \mid -1 \leq x \leq 1\}$

$(n\cdot) : \mathbb{R}^+ \to \mathbb{R}^+$

$T_n : I \to I$



Expanded: $\forall v : \mathbb{R}^+ .\ \cos(n \cdot v) == T_n(\cos v)$

$n=2$: $\cos(2\cdot v) = 2\cdot\cos^2 v - 1 == T_2(\cos v)$

trig. law

$\Rightarrow\ T_2 x = 2x^2 - 1$

generally: $v = \arccos x \ \Rightarrow\ T_n x = \cos(n \cdot \arccos x)$

DSL → δσλ

DSLsofMath

Polynomials & Homomorphisms

Patrik Jansson

Syntax: a list of coefficients

Semantics: a "polynomial" function

```
eval :: [ℝ] → (ℝ→ℝ)
eval []       x = 0
eval (a:as)   x = a + x·(eval as x)
```

We have +, −, ·, 0, 1 on functions ℝ→ℝ (a Ring structure).

Can we find these operations on [ℝ] to make eval a Ring-homomorphism?

Polynomials & Homomorphisms

Patrik Jansson

Syntax: a list of coefficients

Semantics: a "polynomial" function

```
eval :: [ℝ] → (ℝ → ℝ)
eval []       x = 0
eval (a : as) x = a + x · (eval as x)
```

$\exists\, add.\ H_2(eval, add, \oplus)$?

$add : [\mathbb{R}] \to [\mathbb{R}] \to [\mathbb{R}]$

Polynomials & Homomorphisms

Patrik Jansson

Syntax: a list of coefficients

Semantics: a "polynomial" function

```
eval : [ℝ] → (ℝ→ℝ)
eval []       x = 0
eval (a:as)   x = a + x·(eval as x)
```

$\exists add.\ H_2(eval, add, \oplus)$?

```
add : [ℝ] → [ℝ] → [ℝ]
add [] [] = []
add [] bs = bs
add as [] = as
add as bs = core
```

DSL → δσλ

DSLsofMath

Polynomials & Homomorphisms

Patrik Jansson

```
eval : [ℝ] → (ℝ → ℝ)
eval []       x = 0
eval (a : as) x = a + x · (eval as x)
```

$$H_2(eval, add, \oplus) =$$
$$\forall as, bs.\ eval\ (add\ as\ bs) == (eval\ as) \oplus (eval\ bs)$$

Proof by structural induction

with $P(as, bs) = eval\ (add\ as\ bs) == (eval\ as) \oplus (eval\ bs)$

Cases: $P([], [])$, $\forall as.\ P(as, [])$, $\forall bs.\ P([], bs)$,

$\forall a, b, as, bs.\ P(as, bs) \Rightarrow P(a : as, b : bs)$

induction hypothesis (IH)

Conclusion: $\forall as, bs.\ P(as, bs)$

Polynomials & Homomorphisms

Patrik Jansson

```
eval : [ℝ] → (ℝ → ℝ)
eval []     x = 0
eval (a:as) x = a + x·(eval as x)
```

Prove P(a:as, b:bs) (assuming IH)

P(as, bs) = (eval as) ⊕ (eval bs) == eval (add as bs)

induction hypothesis (IH)

```
(eval (a:as) ⊕ eval (b:bs)) x =
 eval (a:as) x  +  eval (b:bs) x        def. of ⊕
(a + x·eval as x) + (b + x·eval bs x)   def. of eval
a+b + x·(eval as x + eval bs x)         Ring laws
(a+b) + x·((eval as ⊕ eval bs) x)       def. of ⊕
(a+b) + x·(eval (add as bs) x)          IH
eval ((a+b):(add as bs)) x              def. of eval
eval (add (a:as) (b:bs)) x              define add
```

core

Polynomials & Homomorphisms

Patrik Jansson

```
eval : [ℝ] → (ℝ→ℝ)
eval []     x = 0
eval (a:as) x = a + x·(eval as x)
```

$$H_2(eval, add, \oplus) =$$
$$\forall as, bs.\ eval(add\ as\ bs) == (eval\ as) \oplus (eval\ bs)$$

```
add []     []     = []
add []     bs     = bs
add as     []     = as
add (a:as) (b:bs) = (a+b) : add as bs
```

core

```
instance Additive [REAL] where (+)=add ; zero=[]
```

DSL → δσλ
DSLsofMath

Polynomials & Homomorphisms

Patrik Jansson

```
eval : [ℝ] → (ℝ → ℝ)
eval []       x = 0
eval (a:as)   x = a + x · (eval as x)
```

Now: add (a:as) (b:bs) = ?

$H_2(\text{eval}, \text{add}, \oplus) =$ IH

$\forall as, bs.\ \text{eval}(\text{add}\ as\ bs) == (\text{eval}\ as) \oplus (\text{eval}\ bs)$

Calculate:

$(\text{eval}(a:as) \oplus \text{eval}(b:bs))\ x =$ -- def. of $\oplus$

$= \text{eval}(a:as)\ x + \text{eval}(b:bs)\ x =$ -- def. of eval

$= (a + x \cdot \text{eval}\ as\ x) + (b + x \cdot \text{eval}\ bs\ x) =$ -- Ring laws

$= (a+b) + x \cdot (\text{eval}\ as\ x + \text{eval}\ bs\ x) =$ -- def. of $\oplus$

$= (a+b) + x \cdot ((\text{eval}\ as) \oplus (\text{eval}\ bs))\ x =$ -- IH

$= (a+b) + x \cdot \text{eval}(\text{add}\ as\ bs)\ x =$ -- def. of eval

$= \text{eval}((a+b) : \text{add}\ as\ bs)\ x$