

# Formally Verified Approximations using certificates

Florent Bréhard, Assia Mahboubi, Damien Pous

Lyon/Toulouse, Nantes, Lyon

ITP, Portland, 10.09.2019



$$\int_0^{\sqrt{2}} \frac{1+t}{\sqrt{\pi+t}} dt$$

# Numbers

$$\pi^2 - \frac{29e}{8}$$

# Numbers

$$\pi^2 - \frac{29e}{8}$$

$$\pi \approx 3.1$$

$$e \approx 2.7$$

$$\pi^2 \approx 9.6$$

$$29e/8 \approx 9.8$$

$$\pi^2 - 29e/8 \approx -0.2$$

# Numbers

$$\pi^2 - \frac{29e}{8}$$

$$\pi \approx 3.14$$

$$e \approx 2.72$$

$$\pi^2 \approx 9.86$$

$$29e/8 \approx 9.86$$

$$\pi^2 - 29e/8 \approx 0.00$$

# Numbers

$$\pi^2 - \frac{29e}{8}$$

$$\pi \approx 3.141$$

$$e \approx 2.718$$

$$\pi^2 \approx 9.866$$

$$29e/8 \approx 9.853$$

$$\pi^2 - 29e/8 \approx 0.013$$

# Numbers

$$\pi^2 - \frac{29e}{8}$$

$$\pi \approx 3.141$$

$$e \approx 2.718$$

$$\pi^2 \approx 9.866$$

$$29e/8 \approx 9.853$$

$$\pi^2 - 29e/8 \approx 0.013$$

$$\pi \in [3.141; 3.142]$$

$$e \in [2.718; 2.719]$$

$$\pi^2 \in [9.865; 9.872]$$

$$29e/8 \in [9.852; 9.857]$$

$$\pi^2 - 29e/8 \in [0.008; 0.020]$$

# Functions

$$x \mapsto e + \sin(x)$$



# Functions

$$x \mapsto e + \sin(x)$$

$$x \mapsto e + x - \frac{1}{6}x^3 + o(x^5)$$

# Functions

$$x \mapsto e + \sin(x)$$

$$x \mapsto e + x - \frac{1}{6}x^3 + o(x^5)$$

$$x \mapsto 2.71 + x - 0.17x^3$$

# Functions

$$x \mapsto e + \sin(x)$$

$$x \mapsto e + x - \frac{1}{6}x^3 + o(x^5)$$

$$x \mapsto 2.71 + x - 0.17x^3$$

$$x \mapsto [2.71; 2.72] + x + [-0.17; -0.16]x^3$$

# Functions

$$x \mapsto e + \sin(x)$$

$$x \mapsto e + x - \frac{1}{6}x^3 + o(x^5)$$

$$x \mapsto 2.71 + x - 0.17x^3$$

$$x \mapsto [2.71; 2.72] + x + [-0.17; -0.16]x^3 + [-0.01; 0.01]$$

(over  $[-1; 1]$ )

# Rigorous Polynomial Approximations

[Berz and Makino '98]

Approximate  $f : \mathbb{R} \rightarrow \mathbb{R}$  by a pair  $(P, \epsilon)$  with

- $P$  a sequence of intervals, the coefficients
- $\epsilon$  an interval, the remainder

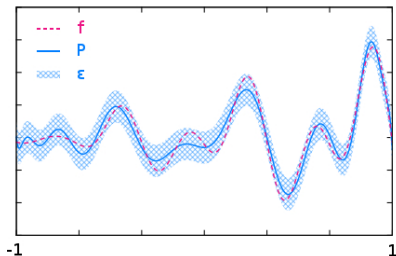
such that

$$\exists p \in P, \forall x, f(x) - p(x) \in \epsilon$$

evaluation of  $p$  at  $x$

a sequence of real coefficients

pointwise containment



# Existing Coq libraries

$\mathbb{R}$	standard library + Coquelicot
$\mathbb{F}$	Flocq
$\mathbb{R}$ approximated by $\mathbb{I}$	CoqInterval
$\mathbb{R}^{\mathbb{R}}$ approximated by $\mathbb{I}^* \times \mathbb{I}$	CoqApprox (“Taylor models”)

## Existing Coq libraries

$\mathbb{R}$	standard library + Coquelicot
$\mathbb{F}$	Flocq
$\mathbb{R}$ approximated by $\mathbb{I}$	CoqInterval
$\mathbb{R}^{\mathbb{R}}$ approximated by $\mathbb{I}^* \times \mathbb{I}$	CoqApprox (“Taylor models”)

idealised operations on  $\mathbb{R}$  reflected by computable operations on  $\mathbb{I}$

idealised operations on  $\mathbb{R}^{\mathbb{R}}$  reflected by computable operations on  $\mathbb{I}^* \times \mathbb{I}$

# Existing Coq libraries

$\mathbb{R}$	standard library + Coquelicot
$\mathbb{F}$	Flocq
$\mathbb{R}$ approximated by $\mathbb{I}$	CoqInterval
$\mathbb{R}^{\mathbb{R}}$ approximated by $\mathbb{I}^* \times \mathbb{I}$	CoqApprox (“Taylor models”)

idealised operations on  $\mathbb{R}$  reflected by computable operations on  $\mathbb{I}$   
idealised operations on  $\mathbb{R}^{\mathbb{R}}$  reflected by computable operations on  $\mathbb{I}^* \times \mathbb{I}$

In this work:

1. new abstraction layers
2. Chebyshev polynomials
3. certificate-based approach for dealing with certain operations



# Polymorphism

```
Record Ops := {  
  car:> Type;  
  add,sub,mul,div: car → car → car;  
  cos,abs,sqrt: car → car;  
  zer,one,pi: car;  
}.
```

Instances for  $\mathbb{R}$ ,  $\mathbb{F}$ ,  $\mathbb{I}$ : ROps, FOps, IOps.

# Polymorphism

```
Record Ops := {  
  car:> Type;  
  add,sub,mul,div: car → car → car;  
  cos,abs,sqrt: car → car;  
  zer,one,pi: car;  
}.
```

Instances for  $\mathbb{R}$ ,  $\mathbb{F}$ ,  $\mathbb{I}$ : ROps, FOps, IOps.

**Definition**  $f(C: \text{Ops}): C \rightarrow C := \text{fun } x \Rightarrow \text{sqrt } (\text{pi} + x * x)$ .

# Polymorphism

```
Record Ops := {  
  car:> Type;  
  add,sub,mul,div: car → car → car;  
  cos,abs,sqrt: car → car;  
  zer,one,pi: car;  
}.
```

Instances for  $\mathbb{R}$ ,  $\mathbb{F}$ ,  $\mathbb{I}$ : ROps, FOps, IOps.

**Definition**  $f(C: \text{Ops}): C \rightarrow C := \text{fun } x \Rightarrow \text{sqrt } (\text{pi} + x * x)$ .

- $f \text{ ROps}: \mathbb{R} \rightarrow \mathbb{R}$                       the idealised function  $x \mapsto \sqrt{\pi + x^2}$
- $f \text{ FOps}: \mathbb{F} \rightarrow \mathbb{F}$                       a floating point implementation
- $f \text{ IOps}: \mathbb{I} \rightarrow \mathbb{I}$                       an interval implementation

# Parametricity

```
Record Rel (C D: 0ps) := {  
  rel:> C → D → Prop;  
  radd: ∀ x y, rel x y → ∀ x' y', rel x' y' → rel (x+x') (y+y');  
  rcos: ∀ x y, rel x y → rel (cos x) (cos y);  
  rzer: rel 0 0;  
  ...  
}.
```

**Lemma** IRel: Rel R0ps I0ps := { rel x X := x ∈ X }.

**Proof.** (\* redirect to CoqInterval \*) Defined.

# Parametricity

```
Record Rel (C D: Ops) := {  
  rel:> C → D → Prop;  
  radd: ∀ x y, rel x y → ∀ x' y', rel x' y' → rel (x+x') (y+y');  
  rcos: ∀ x y, rel x y → rel (cos x) (cos y);  
  rzer: rel 0 0;  
  ...  
}.
```

**Lemma** IRel: Rel ROps IOps := { rel x X := x ∈ X }.

**Proof.** (\* redirect to CoqInterval \*) **Defined.**

**Definition** f(C: Ops): C → C := ...

**Lemma** rf C D (rel: Rel C D): ∀ x y, rel x y → rel (f x) (f y).

**Proof.** (\* automatic \*) **Qed.**

# Parametricity

```
Record Rel (C D: Ops) := {  
  rel:> C → D → Prop;  
  radd: ∀ x y, rel x y → ∀ x' y', rel x' y' → rel (x+x') (y+y');  
  rcos: ∀ x y, rel x y → rel (cos x) (cos y);  
  rzer: rel 0 0;  
  ...  
}.
```

**Lemma** IRel: Rel ROps IOps := { rel x X := x ∈ X }.

**Proof.** (\* redirect to CoqInterval \*) **Defined.**

**Definition** f(C: Ops): C → C := ...

**Lemma** rf C D (rel: Rel C D): ∀ x y, rel x y → rel (f x) (f y).

**Proof.** (\* automatic \*) **Qed.**

**Check** rf IRel: ∀ (x: ℝ) (X: ℐ), x ∈ X → f x ∈ f X.

idealised function

interval implementation

All polymorphic functions are correct by parametricity!

## Generic bases

Approximate  $f : \mathbb{R} \rightarrow \mathbb{R}$  by linear combinations of a family  $(T_n : \mathbb{R} \rightarrow \mathbb{R})_{n \in \mathbb{N}}$

For  $F = (P, \epsilon) \in \mathbb{I}^* \times \mathbb{I}$ , set

$$f \in F \triangleq \exists p \in P, \forall x, f(x) - p[x] \in \epsilon$$

where  $p[x] = \sum_i p_i T_i(x)$

# Generic bases

Approximate  $f : \mathbb{R} \rightarrow \mathbb{R}$  by linear combinations of a family  $(T_n : \mathbb{R} \rightarrow \mathbb{R})_{n \in \mathbb{N}}$

For  $F = (P, \epsilon) \in \mathbb{I}^* \times \mathbb{I}$ , set

$$f \in F \triangleq \exists p \in P, \forall x, f(x) - p[x] \in \epsilon$$

where  $p[x] = \sum_i p_i T_i(x)$

To implement the elementary operations on  $\mathbb{I}^* \times \mathbb{I}$ , we require:

beval:  $\forall C : \text{Ops}, \text{seq } C \rightarrow C \rightarrow C$

bmul:  $\forall C : \text{Ops}, \text{seq } C \rightarrow \text{seq } C \rightarrow \text{seq } C$

bprim:  $\forall C : \text{Ops}, \text{seq } C \rightarrow \text{seq } C$

...

evalE:  $\forall p \ x, \text{beval } p \ x = p[x]$

eval\_mul:  $\forall p \ q \ x, (\text{bmul } p \ q)[x] = p[x] * q[x]$

eval\_prim:  $\forall p \ a \ b, (\text{bprim } p)[b] - (\text{bprim } p)[a] = \text{RInt } (p[_]) \ a \ b$

...

rbeval:  $\forall p \ P, p \in P \rightarrow \forall x \ X, x \in X \rightarrow \text{beval } p \ x \in \text{beval } P \ X$

rbmul:  $\forall p \ P, p \in P \rightarrow \forall q \ Q, q \in Q \rightarrow \text{bmul } p \ q \in \text{bmul } P \ Q$

rbprim:  $\forall p \ P, p \in P \rightarrow \text{bprim } p \in \text{bprim } P$

...

polymorphic, base-specific, operations

adequacy with  $T$  on  $\mathbb{R}$

parametricity



## Chebyshev basis

$$T_0 = 1$$

$$T_1 = X$$

$$T_{n+2} = 2XT_{n+1} - T_n$$

# Chebyshev basis

$$T_0 = 1 \qquad T_1 = X \qquad T_{n+2} = 2XT_{n+1} - T_n$$

```
Fixpoint Clenshaw (C: 0ps) b c (p: seq C) x :=  
  match p with  
  | [] => c - x*b  
  | a::q => Clenshaw c (a + 2*x*c - b) q x  
  end.
```

```
Definition beval (C: 0ps) (p: seq C) x := Clenshaw 0 0 (rev p) x.
```

# Chebyshev basis

$$T_0 = 1 \qquad T_1 = X \qquad T_{n+2} = 2XT_{n+1} - T_n$$

```
Fixpoint Clenshaw (C: 0ps) b c (p: seq C) x :=
  match p with
  | [] => c - x*b
  | a::q => Clenshaw c (a + 2*x*c - b) q x
  end.
```

**Definition** beval (C: 0ps) (p: seq C) x := Clenshaw 0 0 (rev p) x.

**Lemma** ClenshawE b c p x: Clenshaw b c p x = (catrev p [c - 2\*x\*b; b])[x]

**Proof.**

```
  revert b c; induction p as [|a p IH]; intros.
+ compute. rewrite !T0 !T1 /=. ring.
+ rewrite /=IH/= 2!catrevE 2!eval_app /=TSS/=. ring.
```

**Qed.**

**Lemma** rClenshaw C D (T: Rel C D):

$\forall p q, T p q \rightarrow \forall a b, T a b \rightarrow$

$\forall c d, T c d \rightarrow \forall x y, T x y \rightarrow T (\text{Clenshaw } a \ c \ p \ x) (\text{Clenshaw } b \ d \ q \ y)$

**Proof.** induction 1; parametricity. **Qed.**

## So far

- abstraction w.r.t. 1/ intervals and 2/ approximation basis
- two concrete bases: monomial (Taylor) and Chebyshev
- writing  $\mathbb{M}$  for  $\mathbb{I}^* \times \mathbb{I}$ , we have the following functions:

`const:  $\mathbb{I} \rightarrow \mathbb{M}$`

`id:  $\mathbb{M}$`

`add,sub,mul:  $\mathbb{M} \rightarrow \mathbb{M} \rightarrow \mathbb{M}$`

`eval:  $\mathbb{M} \rightarrow \mathbb{I} \rightarrow \mathbb{I}$`

`prim:  $\mathbb{M} \rightarrow \mathbb{M}$`

`integrate:  $\mathbb{M} \rightarrow \mathbb{I} \rightarrow \mathbb{I} \rightarrow \mathbb{I}$`

`truncate:  $\text{nat} \rightarrow \mathbb{M} \rightarrow \mathbb{M}$`

- what about `div:  $\mathbb{M} \rightarrow \mathbb{M} \rightarrow \mathbb{M}$`  and `sqrt:  $\mathbb{M} \rightarrow \mathbb{M}$` ?  
(those cannot be defined in a polymorphic way!)

# Newton-like methods, Oracles, Certificates

## Digression on $\sqrt{2}$ : Newton method

$$\sqrt{2}$$

## Digression on $\sqrt{2}$ : Newton method

$$\sqrt{2}$$

- unique positive root of  $h(x) \triangleq x^2 - 2$
- unique positive fixpoint of  $t(x) \triangleq x - \frac{h(x)}{h'(x)} \left( = \frac{x^2+2}{2x} \right)$
- $t(1) = 1.5$   
 $t^2(1) \approx 1.4167$   
 $t^3(1) \approx 1.4142157$   
...

# Banach Fixpoint Theorem — global statement

Let  $(X, d)$  be a **complete** metric space, and  $\mathbf{T} : X \rightarrow X$ .  
If  $\mathbf{T}$  is  **$\mu$ -Lipschitz** for some  $\mu \in [0, 1)$ , i.e.,

$$\forall x, y \in X, \quad d(\mathbf{T}x, \mathbf{T}y) \leq \mu d(x, y) ,$$

then  $\mathbf{T}$  admits a **unique fixpoint**  $x^*$  and for all  $x^\circ \in X$  we have

$$\frac{d(x^\circ, \mathbf{T}x^\circ)}{1 + \mu} \leq d(x^\circ, x^*) \leq \frac{d(x^\circ, \mathbf{T}x^\circ)}{1 - \mu} .$$



## Digression on $\sqrt{2}$ : oracles and validation

$$\sqrt{2}$$

- unique positive root of  $h(x) \triangleq x^2 - 2$
- unique positive fixpoint of  $t(x) \triangleq x - \frac{h(x)}{h'(x)} \left( = \frac{x^2+2}{2x} \right)$

## Digression on $\sqrt{2}$ : oracles and validation

$$\sqrt{2}$$

- unique positive root of  $h(x) \triangleq x^2 - 2$
- unique positive fixpoint of  $t(x) \triangleq x - \frac{h(x)}{h'(x)} \left( = \frac{x^2+2}{2x} \right)$
- $t$  is contracting on  $[1.4; 1.5]$  with Lipschitz factor  $\mu = 0.12$

→ for all  $x^\circ \in [1.4; 1.5]$ ,  $|\sqrt{2} - x^\circ| \leq \frac{x^\circ - t(x^\circ)}{1-0.12}$

# Banach Fixpoint Theorem — local statement

Let  $(X, d)$  be a complete metric space,  $\mathbf{T} : X \rightarrow X$ ,  $x^\circ \in X$ , and  $\mu, b, r \in \mathbb{R}_+$ . Let  $\bar{B}(x^\circ, r)$  be the ball  $\{x \in X \mid d(x^\circ, x) \leq r\}$ .

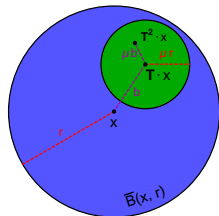
If

- $\mathbf{T}$  is  $\mu$ -Lipschitz over  $\bar{B}(x^\circ, r)$ :

$$\forall x, y \in \bar{B}(x^\circ, r), d(\mathbf{T}x, \mathbf{T}y) \leq \mu d(x, y) ,$$

- $d(x^\circ, \mathbf{T}x^\circ) \leq b$ ,  $\mu < 1$ , and  $b + \mu r \leq r$ ,

then  $\mathbf{T}$  admits a unique fixpoint  $x^*$  in  $\bar{B}(x^\circ, r)$ .



# Banach Fixpoint Theorem — local statement

Let  $(X, d)$  be a complete metric space,  $\mathbf{T} : X \rightarrow X$ ,  $x^\circ \in X$ , and  $\mu, b, r \in \mathbb{R}_+$ . Let  $\bar{B}(x^\circ, r)$  be the ball  $\{x \in X \mid d(x^\circ, x) \leq r\}$ .

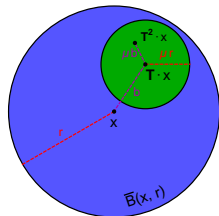
If

- $\mathbf{T}$  is  $\mu$ -Lipschitz over  $\bar{B}(x^\circ, r)$ :

$$\forall x, y \in \bar{B}(x^\circ, r), d(\mathbf{T}x, \mathbf{T}y) \leq \mu d(x, y) ,$$

- $d(x^\circ, \mathbf{T}x^\circ) \leq b$ ,  $\mu < 1$ , and  $b + \mu r \leq r$ ,

then  $\mathbf{T}$  admits a unique fixpoint  $x^*$  in  $\bar{B}(x^\circ, r)$ .



**Proof.**

(\* using filter-based topology from Coquelicot \*)

(\* shorter/simpler than existing proofs \*)

**Qed.**

## Certificates for division

- $f/g$  unique root of **affine** operator  $\mathbf{F} : h \mapsto gh - f$
- $\mathcal{D}\mathbf{F}_h : k \mapsto gk \quad \Rightarrow \quad (\mathcal{D}\mathbf{F}_h)^{-1} \approx k \mapsto wk \quad \text{with} \quad w \approx 1/g$

$$\mathbf{T} : h \mapsto h - w(gh - f)$$

## Certificates for division

- $f/g$  unique root of **affine** operator  $\mathbf{F} : h \mapsto gh - f$
- $\mathcal{D}\mathbf{F}_h : k \mapsto gk \Rightarrow (\mathcal{D}\mathbf{F}_h)^{-1} \approx k \mapsto wk$  with  $w \approx 1/g$

$$\mathbf{T} : h \mapsto h - w(gh - f)$$

### Proposition

Let  $f, g, h^\circ, w \in \mathcal{C}(I)$  and  $\mu, b \in \mathbb{R}_+$  such that

$$\|w(gh^\circ - f)\| \leq b \qquad \|1 - wg\| \leq \mu < 1$$

Then  $g$  does not vanish over  $I$  and  $\|h^\circ - f/g\| \leq \frac{b}{1-\mu}$ .

## Certificates for division

- $f/g$  unique root of **affine** operator  $\mathbf{F} : h \mapsto gh - f$
- $\mathcal{D}\mathbf{F}_h : k \mapsto gk \Rightarrow (\mathcal{D}\mathbf{F}_h)^{-1} \approx k \mapsto wk$  with  $w \approx 1/g$

$$\mathbf{T} : h \mapsto h - w(gh - f)$$

### Proposition

Let  $f, g, h^\circ, w \in \mathcal{C}(I)$  and  $\mu, b \in \mathbb{R}_+$  such that

$$\|w(gh^\circ - f)\| \leq b \qquad \|1 - wg\| \leq \mu < 1$$

Then  $g$  does not vanish over  $I$  and  $\|h^\circ - f/g\| \leq \frac{b}{1-\mu}$ .

### Proof.

- $\|\mathcal{D}\mathbf{T}_h\| = \|1 - wg\| \leq \mu \Rightarrow \mathbf{T}$  is  $\mu$ -Lipschitz
- $\|h^\circ - \mathbf{T} \cdot h^\circ\| = \|w(gh^\circ - f)\| \leq b$

$\Rightarrow$  Apply Banach fixpoint theorem (global statement) □

## Certificates for Square Root

- $\sqrt{f}$  is the positive root of **quadratic** operator  $\mathbf{F} : h \mapsto h^2 - f$
- $\mathcal{D}\mathbf{F}_h : k \mapsto 2hk$ ,  $(\mathcal{D}\mathbf{F}_{h^\circ})^{-1} \approx k \mapsto wk$  with  $w \approx 1/2h^\circ$   
 $\mathbf{T} : h \mapsto h - w(h^2 - f)$



## Certificates for Square Root

- $\sqrt{f}$  is the positive root of **quadratic** operator  $\mathbf{F} : h \mapsto h^2 - f$
- $\mathcal{DF}_h : k \mapsto 2hk$ ,  $(\mathcal{DF}_{h^\circ})^{-1} \approx k \mapsto wk$  with  $w \approx 1/2h^\circ$   
 $\mathbf{T} : h \mapsto h - w(h^2 - f)$

### Proposition

Let  $f, h^\circ, w \in \mathcal{C}(I)$ ,  $\mu_0, \mu_1, b \in \mathbb{R}_+$  and  $t_0 \in I$  such that

$$\|w(h^{\circ 2} - f)\| \leq b \quad \|1 - 2wh^\circ\| \leq \mu_0 < 1 \quad \|w\| \leq \mu_1$$

$$(1 - \mu_0)^2 - 8b\mu_1 \geq 0 \quad w(t_0) > 0$$

Then  $f > 0$  over  $I$  and  $\|h^\circ - \sqrt{f}\| \leq \frac{1 - \mu_0 - \sqrt{(1 - \mu_0)^2 - 8b\mu_1}}{4\mu_1}$ .

## Certificates for Square Root

- $\sqrt{f}$  is the positive root of **quadratic** operator  $\mathbf{F} : h \mapsto h^2 - f$
- $\mathcal{DF}_h : k \mapsto 2hk$ ,  $(\mathcal{DF}_{h^\circ})^{-1} \approx k \mapsto wk$  with  $w \approx 1/2h^\circ$   
 $\mathbf{T} : h \mapsto h - w(h^2 - f)$

### Proposition

Let  $f, h^\circ, w \in \mathcal{C}(I)$ ,  $\mu_0, \mu_1, b \in \mathbb{R}_+$  and  $t_0 \in I$  such that

$$\|w(h^{\circ 2} - f)\| \leq b \quad \|1 - 2wh^\circ\| \leq \mu_0 < 1 \quad \|w\| \leq \mu_1$$
$$(1 - \mu_0)^2 - 8b\mu_1 \geq 0 \quad w(t_0) > 0$$

Then  $f > 0$  over  $I$  and  $\|h^\circ - \sqrt{f}\| \leq \frac{1 - \mu_0 - \sqrt{(1 - \mu_0)^2 - 8b\mu_1}}{4\mu_1}$ .

### Proof ultra sketch.

- $\mathbf{T}$  is  $\mu(r)$ -Lipschitz over  $\bar{B}(h^\circ, r)$  for  $\mu(r) := \mu_0 + 2\mu_1 r$
- get optimal solution to  $b + \mu(r)r \leq r$  and apply local Banach fixpoint theorem □

## Oracles

From  $f \in F$ ,  $g \in G$  (with  $f, g : \mathbb{R} \rightarrow \mathbb{R}$ ;  $F, G : \mathbb{M}$ ), guess good approximations of  $f/g$ ,  $1/g$ ,  $\sqrt{f}$ ,  $1/2\sqrt{f}$ , as polynomials with floating point coefficients

# Oracles

From  $f \in F$ ,  $g \in G$  (with  $f, g : \mathbb{R} \rightarrow \mathbb{R}$ ;  $F, G : \mathbb{M}$ ), guess good approximations of  $f/g$ ,  $1/g$ ,  $\sqrt{f}$ ,  $1/2\sqrt{f}$ , as polynomials with floating point coefficients

!!!These computations do not need to be trusted!!!

- do it with your favourite numerical tool, in Fortran77, javascript. . .

# Oracles

From  $f \in F$ ,  $g \in G$  (with  $f, g : \mathbb{R} \rightarrow \mathbb{R}$ ;  $F, G : \mathbb{M}$ ), guess good approximations of  $f/g$ ,  $1/g$ ,  $\sqrt{f}$ ,  $1/2\sqrt{f}$ , as polynomials with floating point coefficients

!!!These computations do not need to be trusted!!!

- do it with your favourite numerical tool, in Fortran77, javascript. . .

we chose Coq. . .

# Oracles

From  $f \in F$ ,  $g \in G$  (with  $f, g : \mathbb{R} \rightarrow \mathbb{R}$ ;  $F, G : \mathbb{M}$ ), guess good approximations of  $f/g$ ,  $1/g$ ,  $\sqrt{f}$ ,  $1/2\sqrt{f}$ , as polynomials with floating point coefficients

!!!These computations do not need to be trusted!!!

- do it with your favourite numerical tool, in Fortran77, javascript...

we chose Coq...

- we use Discrete Cosine Transform (DCT)  
(we should actually do fast DCT, in  $O(n \log(n))$ )
- i.e., interpolation at Chebyshev nodes of the first kind

$$\mu_k^{(n)} = \cos\left(\frac{(k - 1/2)\pi}{n}\right) \quad k \in [1..n]$$

- we evaluate  $f/g$ ,  $1/g$ ... at those points using the models  $F$ ,  $G$  and floating point arithmetics (reusing the polymorphic `beval` function, applied to the unspecified `F0ps` instance)

## Last bit for validation

We need to majorise values such as  $\|w(gh^\circ - f)\|$

Since we have models  $W, G, H^\circ, F$  for  $w, g, h^\circ, f$ , it suffices to know how to majorise  $\|M\|$  for arbitrary models  $M : \mathbb{M}$

In Chebyshev basis, on  $[-1; 1]$ , we have  $|T_n(x)| \leq 1$  since  $T_n(\cos t) = \cos(nt)$ , so that we can take the sum of the absolute values of the coefficients

# Summary

We have functions with the following types, with the obvious specification w.r.t. their counterparts on (idealised) real numbers

`const`:  $\mathbb{I} \rightarrow \mathbb{M}$

`id`:  $\mathbb{M}$

`add, sub, mul`:  $\mathbb{M} \rightarrow \mathbb{M} \rightarrow \mathbb{M}$

`eval`:  $\mathbb{M} \rightarrow \mathbb{I} \rightarrow \mathbb{I}$

`prim`:  $\mathbb{M} \rightarrow \mathbb{M}$

`integrate`:  $\mathbb{M} \rightarrow \mathbb{I} \rightarrow \mathbb{I} \rightarrow \mathbb{I}$

`truncate`:  $\text{nat} \rightarrow \mathbb{M} \rightarrow \mathbb{M}$

`sqrt`:  $\text{nat} \rightarrow \mathbb{M} \rightarrow \mathbb{M}$

`div`:  $\text{nat} \rightarrow \mathbb{M} \rightarrow \mathbb{M} \rightarrow \mathbb{M}$

- ⇒ certified approximations for all numbers and functions expressible from those constructs:
- example from the first slide
  - Hilbert's 16th problem: computing integrals for  $\mathcal{H}(4) \geq 24$



## Future work

- integration with CoqApprox
- delegate oracle computations to external tools
- certificates for the general case of LODE

Florent already did it both on paper and in C!

- other bases?
  - non-polynomial ones, e.g., Bessel functions
  - unbounded domains: Laguerre, Hermite

## Future work

- integration with CoqApprox
- delegate oracle computations to external tools
- certificates for the general case of LODE

Florent already did it both on paper and in C!

- other bases?
  - non-polynomial ones, e.g., Bessel functions
  - unbounded domains: Laguerre, Hermite

Thanks!



Florent Bréhard - Nicolas Brisebarre - Mioara Joldes - Assia Mahboubi