Formally Verified Approximations

using certificates

Florent Bréhard, Louis Gaillard, Assia Mahboubi, Damien Pous

Nuscap, Toulouse, o9.o6.2o22

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

Numbers

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

Numbers

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

$$\pi \approx 3.1 \qquad \pi^2 \approx 9.6$$

$$e \approx 2.7 \qquad 29e/8 \approx 9.8$$

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

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

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

$$\pi \approx 3.141 \qquad \pi^2 \approx 9.866$$

$$e \approx 2.718 \qquad 29e/8 \approx 9.853$$

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

Numbers

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

$$\pi \approx 3.141 \qquad \pi^2 \approx 9.866$$
$$e \approx 2.718 \qquad 29e/8 \approx 9.853$$
$$\pi^2 - 29e/8 \approx 0.013$$

$$\pi \in [3.141; 3.142] \qquad \pi^2 \in [9.865; 9.872]$$
$$e \in [2.718; 2.719] \qquad 29e/8 \in [9.852; 9.857]$$
$$\pi^2 - 29e/8 \in [0.008; 0.020]$$

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

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

$$\begin{aligned} x &\mapsto e + x - \frac{1}{6}x^3 + O(x^5) \\ x &\mapsto 2.71 + x - 0.17x^3 \\ x &\mapsto [2.71; 2.72] + x + [-0.17; -0.16]x^3 \end{aligned}$$

Functions

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

$$\begin{aligned} x &\mapsto e + x - \frac{1}{6}x^3 + O(x^5) \\ x &\mapsto 2.71 + x - 0.17x^3 \\ x &\mapsto [2.71; 2.72] + x + [-0.17; -0.16]x^3 + [-0.01; 0.01] \end{aligned}$$

(over $[-1; 1]$)

Rigorous Polynomial Approximations

[Berz and Makino '98]

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

- P a sequence of intervals, the coefficients
- ϵ an interval, the remainder

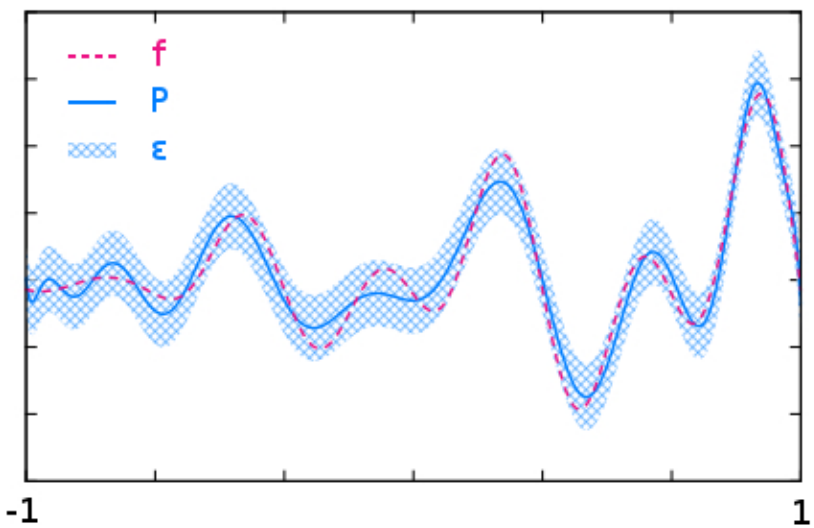
such that

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

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 & Fourier series
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: Ops): C→C := fun x => sqrt (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: Ops): C→C := fun x => sqrt (pi+x*x).
```

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

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.
```

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!

More on interval abstraction

```
Class NBH := {
  (** intervals (with +,*,/,-,sqrt,cos,pi,1,0) *)
  II: Ops1;
  (** (parametric) containment relation *)
  contains: Rel1 II ROps1;

  (** convexity of intervals  *)
  convex: ∀ Z x y, x ∈ Z → y ∈ Z → ∀ z, x≤z≤y → z ∈ Z;

  (** additional operations on intervals *)
  bnd: II → II → II;
  min,max: II → option II;
  bot: II;                        (** [[-oo;+oo]] *)
  is_lt, is_le: II → II → bool;

  (** specification of the above operations *)
  bndE: ∀ x y X Y, x ∈ X → y ∈ Y → ∀ z, x≤z≤y → z ∈ bnd X Y;
  ...

  (** unspecified floating point operations *)
  FF: Ops1;
  I2F: II → FF;
  F2I: FF → II;
}.
```

Approximations in a generic base

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

For a sequence p of coefficients, write $p[x] = \sum_i p_i T_i(x)$.

Approximations in a generic base

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

For a sequence p of coefficients, write $p[x] = \sum_i p_i T_i(x)$.

To implement rigorous approximations in such a base, we require:

```
beval: ∀ C: Ops, seq C → C → C
bmul: ∀ C: Ops, seq C → seq C → seq C
bint: ∀ C: Ops, seq C → C → C → seq C
...
evalE: ∀ p x, beval p x = p[x]
eval_mul: ∀ p q x, (bmul p q)[x] = p[x] * q[x]
eval_int: ∀ p a b, bint p a b = RInt (p[_]) a b
...
rbeval: p ∈ P → x ∈ X → beval p x ∈ beval P X
rbmul: p ∈ P → q ∈ Q → bmul p q ∈ bmul P Q
rbint: p ∈ P → a ∈ A → b ∈ B → bint p a b ∈ bint P A B
...
```

polymorphic, base-specific, operations

adequacy with T on $\mathbb{R}$

parametricity

Chebyshev basis

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

Chebyshev basis

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

```
Fixpoint Clenshaw (C: Ops) 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: Ops) (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: Ops) 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: Ops) (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):
 ∀ p q, T p q → ∀ a b, T a b →
 ∀ c d, T c d → ∀ x y, T x y → T (Clenshaw a c p x) (Clenshaw b d q y)
Proof. induction 1; parametricity. Qed.
```

Chebyshev basis (continued)

```
Definition pmul (C: Ops) (p q: seq C): seq C := ...
Definition prim (C: Ops) (p: seq C): seq C := ...

(* mathematical correctness, in R *)

(* parametricity *)
```

Rigorous approximations

Given an abstract basis (family of functions + basic functions), we construct models and their basic operations

Mathematically, set $\mathbb{M} \triangleq \mathbb{I}^* \times \mathbb{I}$, ("models", "tubes")
in Coq:

```
Record Tube := { pol: list II; rem: II }.
```

Rigorous approximations

Given an abstract basis (family of functions + basic functions), we construct models and their basic operations

Mathematically, set $\mathbb{M} \triangleq \mathbb{I}^* \times \mathbb{I}$, ("models", "tubes")
in Coq:

```
Record Tube := { pol: list II; rem: II }.

Definition madd (F G: Tube): Tube :=
{| pol := pol F + pol G;
   rem := rem F + rem G |}.
Definition msub (F G: Tube): Tube :=
{| pol := pol F - pol F;
   rem := rem F - rem G |}.
Definition mint (F: Tube) (A B: II): II :=
   bint (pol F) A B + (B-A)*rem F.
```

Multiplication?

```
Definition mmul (F G: Tube): Tube :=
{| pol := pol F * pol G;
   rem := ??? |}.
```

Multiplication?

```
Definition mmul (F G: Tube): Tube :=
{| pol := pol F * pol G;
   rem := ??? |}.
```

Requires a (good) way of computing the range of linear combinations of the given family...

Rigorous approximations

For $f : \mathbb{R} \to \mathbb{R}$ and $F = (P, \epsilon) \in \mathbb{M}$, set

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

We prove lemmas such as:

```
Lemma: f∈F → g∈G → f+g ∈ madd F G.
Lemma: f∈F → g∈G → f-g ∈ msub F G.
Lemma: f∈F → g∈G → f*g ∈ mmul F G.
Lemma: f∈F → a∈A → b∈B → RInt f a b ∈ mint F A B.
```

So far

- abstraction w.r.t. 1/ intervals and 2/ approximation basis
- two concrete bases: monomial (Taylor) and Chebyshev
- we have the following functions, with smooth specifications:

  `const`: $\mathbb{I} \to \mathbb{M}$
  `id`: $\mathbb{M}$
  `add,sub,mul`: $\mathbb{M} \to \mathbb{M} \to \mathbb{M}$
  `eval`: $\mathbb{M} \to \mathbb{I} \to \mathbb{I}$
  `int`: $\mathbb{M} \to \mathbb{I} \to \mathbb{I} \to \mathbb{I}$
  `truncate`: `nat` $\to \mathbb{M} \to \mathbb{M}$

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

Newton-like methods, Oracles, Certificates

Digression on $\sqrt{2}$: Newton's method

$$\sqrt{2}$$

Digression on $\sqrt{2}$: Newton's 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 $\mathbf{T} : X \to X$.
If $\mathbf{T}$ is μ-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

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

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 $\mu = 0.12$

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

Banach Fixpoint Theorem — local statement

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

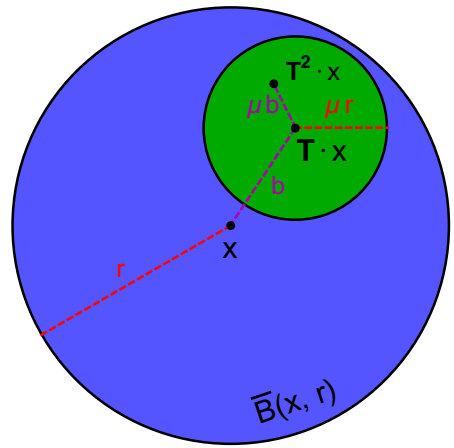
If

- $\mathbf{T}$ is μ-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

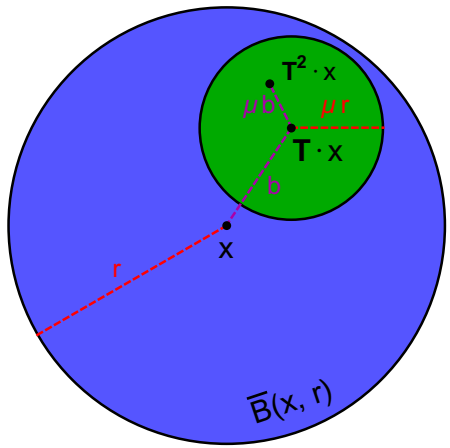
Let (X, d) be a complete metric space, $\mathbf{T} : X \to X$, $x^\circ \in X$, and $\mu, b, r \in \mathbb{R}_+$. Let $\bar{B}(x^\circ, r)$ be the ball $\{x \in X \mid d(x^\circ, x) \leq r\}$.

If

- $\mathbf{T}$ is μ-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 $\mathbf{F} : h \mapsto gh - f$
- $\mathcal{D}\mathbf{F}_h : k \mapsto gk \quad \Rightarrow \quad (\mathcal{D}\mathbf{F}_h)^{-1} \approx k \mapsto wk \quad$ with $\quad w \approx 1/g$

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

Certificates for division

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

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

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

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

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.

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

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

Certificates for Square Root

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

$$\mathbf{T} : h \mapsto h - w(h^2 - f)$$

Certificates for Square Root

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

$$\mathbf{T} : h \mapsto h - w(h^2 - f)$$

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

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

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

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

Certificates for Square Root

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

$$\mathbf{T} : h \mapsto h - w(h^2 - f)$$

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

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

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

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

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 $\square$

Oracles

From $f \in F$, $g \in G$ (with $f, g : \mathbb{R} \to \mathbb{R}$; $F, G : \mathbb{M}$), 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 $f, g : \mathbb{R} \to \mathbb{R}$; $F, G : \mathbb{M}$), 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 $f, g : \mathbb{R} \to \mathbb{R}$; $F, G : \mathbb{M}$), 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 $f, g : \mathbb{R} \to \mathbb{R}$; $F, G : \mathbb{M}$), 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

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

- 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 `FOps` instance)

Last bit for validation

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

Since we have models W, G, H°, F for w, g, h°, 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`: $\mathbb{I} \to \mathbb{M}$
`id`: $\mathbb{M}$
`add,sub,mul`: $\mathbb{M} \to \mathbb{M} \to \mathbb{M}$
`eval`: $\mathbb{M} \to \mathbb{I} \to \mathbb{I}$
`prim`: $\mathbb{M} \to \mathbb{M}$
`integrate`: $\mathbb{M} \to \mathbb{I} \to \mathbb{I} \to \mathbb{I}$
`truncate`: $\texttt{nat} \to \mathbb{M} \to \mathbb{M}$
`sqrt`: $\texttt{nat} \to \mathbb{M} \to \mathbb{M}$
`div`: $\texttt{nat} \to \mathbb{M} \to \mathbb{M} \to \mathbb{M}$

$\Rightarrow$ certified approximations for all numbers and functions expressible from those constructs

Additions by Louis Gaillard

- Fourier series ($F_{2n} = cos(nt),\ F_{2n+1} = sin(nt)$)
  - efficient evaluation, multiplication, range, integration
  - interpolation

  $\Rightarrow$ adds `cos` and `sin` to the language covered by the previous tactic
- Certificates for solutions of polynomial functional equations
  - For a sequence of functions $(h_i : \mathbb{R} \to \mathbb{R})_{i \leq n}$, find a solution $f : \mathbb{R} \to \mathbb{R}$ to

$$\sum_i h_i f^i = 0$$

  - Again via local Banach fixpoint theorem
  - The oracle must also provide a good radius

  $\Rightarrow$ to be used to certify bounds related to Hilbert' 16th problem

Future work

- integration with CoqApprox?
- delegate oracle computations to external tools
- multiplication via FCT/FFT
- other basic functions (`exp` etc)
- 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
- multiplication via FCT/FFT
- other basic functions (`exp` etc)
- 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! Especially to

Florent Bréhard - Nicolas Brisebarre - Louis Gaillard
Mioara Joldes - Assia Mahboubi - Guillaume Melquiond