Formal Methods in Mathematics
Carnegie Mellon University

A Coq Formalization of Lebesgue Integration of Nonnegative Functions

Sylvie Boldo

Inria, Université Paris-Saclay

January 7th, 2020

Disclaimers

Disclaimer 1: this is joint work with

- François Clément,
- Florian Faissole,
- Vincent Martin,
- Micaela Mayero.

Disclaimers

Disclaimer 1: this is joint work with

- François Clément,
- Florian Faissole,
- Vincent Martin,
- Micaela Mayero.

Disclaimer 2:
This formalization of mathematics is done in Coq.

Disclaimers

Disclaimer 1: this is joint work with

- François Clément,
- Florian Faissole,
- Vincent Martin,
- Micaela Mayero.

Disclaimer 2:
This formalization of mathematics is done in Coq.

Disclaimer 3:
There is (nearly) no computer arithmetic!

Outline

Introduction

$\mathfrak{Mathematics}$

$\mathbb{R}$, $\int$, $\frac{\partial^2 u}{\partial t^2}$

theorems

$\mathfrak{Mathematics}$

$\mathbb{R}$, $\int$, $\frac{\partial^2 u}{\partial t^2}$
theorems

Applied Mathematics

numerical scheme, convergence
algorithms + theorems

Introduction

Mathematics	$\mathbb{R}$, $\int$, $\frac{\partial^2 u}{\partial t^2}$ theorems
Applied Mathematics	numerical scheme, convergence algorithms + theorems
Computer	floating-point numbers, implementation programs + ?

Mathem

$\mathbb{R}$, $\int$, $\frac{\partial^2 u}{\partial t^2}$

theorems

Applied

me, convergence

Computer

entation

program

PARANOIA

Motivations

PDE (Partial Differential Equation) $\Rightarrow$ weather forecast
$\Rightarrow$ nuclear simulation
$\Rightarrow$ optimal control
$\Rightarrow$ ...

Motivations

PDE (Partial Differential Equation) $\Rightarrow$ weather forecast
$\Rightarrow$ nuclear simulation
$\Rightarrow$ optimal control
$\Rightarrow$ ...

Usually too complex to solve by an exact mathematical formula
$\Rightarrow$ approximated by numerical scheme over discrete grids/volumes

$\Rightarrow$ mathematical proofs of the convergence of the numerical scheme
(we compute something close to the PDE solution if the size decreases)

Motivations

PDE (Partial Differential Equation) $\Rightarrow$ weather forecast
$\Rightarrow$ nuclear simulation
$\Rightarrow$ optimal control
$\Rightarrow$ ...

Usually too complex to solve by an exact mathematical formula
$\Rightarrow$ approximated by numerical scheme over discrete grids/volumes

$\Rightarrow$ mathematical proofs of the convergence of the numerical scheme
(we compute something close to the PDE solution if the size decreases)

$\Rightarrow$ real program implementing the scheme/method

Motivations

PDE (Partial Differential Equation) $\Rightarrow$ weather forecast
$\Rightarrow$ nuclear simulation
$\Rightarrow$ optimal control
$\Rightarrow$ ...

Usually too complex to solve by an exact mathematical formula
$\Rightarrow$ approximated by numerical scheme over discrete grids/volumes

$\Rightarrow$ mathematical proofs of the convergence of the numerical scheme
(we compute something close to the PDE solution if the size decreases)

$\Rightarrow$ real program implementing the scheme/method

Let us machine-check this kind of programs!

Outline

Motivations

http://www.ima.umn.edu/~arnold/disasters/sleipner.html

The sinking of the Sleipner A offshore platform

Excerpted from a report of SINTEF, Civil and Environmental Engineering:

The Sleipner A platform produces oil and gas in the North Sea and is supported on the seabed at a water depth of 82 m. It is a Condeep type platform with a concrete gravity base structure consisting of 24 cells and with a total base area of 16 000 m^2. Four cells are elongated to shafts supporting the platform deck. The first concrete base structure for Sleipner A sprang a leak and sank under a controlled ballasting operation during preparation for deck mating in Gandsfjorden outside Stavanger, Norway on 23 August 1991.

Immediately after the accident, the owner of the platform, Statoil, a Norwegian oil company appointed an investigation group, and SINTEF was contracted to be the technical advisor for this group.

The investigation into the accident is described in 16 reports...

The conclusion of the investigation was that the loss was caused by a failure in a cell wall, resulting in a serious crack and a leakage that the pumps were not able to cope with. The wall failed as a result of a combination of a serious error in the finite element analysis and insufficient anchorage of the reinforcement in a critical zone.

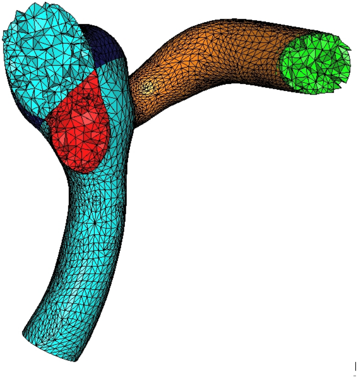
A better idea of what was involved can be obtained from this photo and sketch of the platform. The top deck weighs 57,000 tons, and provides accommodation for about 200 people and support for drilling equipment weighing about 40,000 tons. When the first model sank in August 1991, the crash

Motivations

Real life applications need solving PDE (Partial Differential Equation) on complex 3D geometries.

Motivations

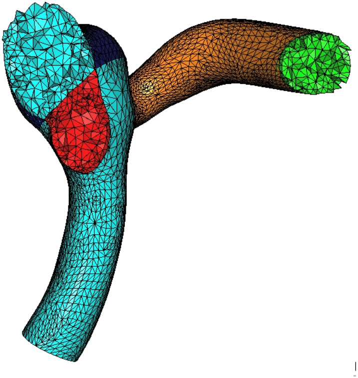
Real life applications need solving PDE (Partial Differential Equation) on complex 3D geometries.



© V. Martin

Motivations

Real life applications need solving PDE (Partial Differential Equation) on complex 3D geometries.



© V. Martin

Instead of regular 2D/3D grids, we consider meshes made of triangles/tetrahedra.

Motivations

The Finite Element Method (FEM) is the most used method to solve PDEs over meshes.

> *FEM encompasses methods for connecting many simple element equations over many small subdomains, named finite elements, to approximate a more complex equation over a larger domain.*
>
> (https://en.wikipedia.org/wiki/Finite_element_method)

Motivations

The Finite Element Method (FEM) is the most used method to solve PDEs over meshes.

> *FEM encompasses methods for connecting many simple element equations over many small subdomains, named finite elements, to approximate a more complex equation over a larger domain.*
>
> (https://en.wikipedia.org/wiki/Finite_element_method)

$\Rightarrow$ mathematical proofs of the FEM
$\Rightarrow$ C++ library (Felisce) implementing the FEM

Motivations

The Finite Element Method (FEM) is the most used method to solve PDEs over meshes.

> *FEM encompasses methods for connecting many simple element equations over many small subdomains, named finite elements, to approximate a more complex equation over a larger domain.*
>
> (`https://en.wikipedia.org/wiki/Finite_element_method`)

⇒ mathematical proofs of the FEM
⇒ C++ library (Felisce) implementing the FEM

Let us machine-check this program!

Motivations

The Finite Element Method (FEM) is the most used method to solve PDEs over meshes.

> *FEM encompasses methods for connecting many simple element equations over many small subdomains, named finite elements, to approximate a more complex equation over a larger domain.*
>
> (https://en.wikipedia.org/wiki/Finite_element_method)

$\Rightarrow$ mathematical proofs of the FEM
$\Rightarrow$ C++ library (Felisce) implementing the FEM

Let us machine-check this program!

First, let us understand/formally prove the mathematics.

Mathematicians at work for Lax-Milgram theorem

- more 50 pages of mathematical proofs

Mathematicians at work for Lax-Milgram theorem

- more 50 pages of mathematical proofs
- very detailed!

Mathematicians at work for Lax-Milgram theorem

- more 50 pages of mathematical proofs
- very detailed!
- more than 7,000 lines and 220,000 characters

Mathematicians at work for Lax-Milgram theorem

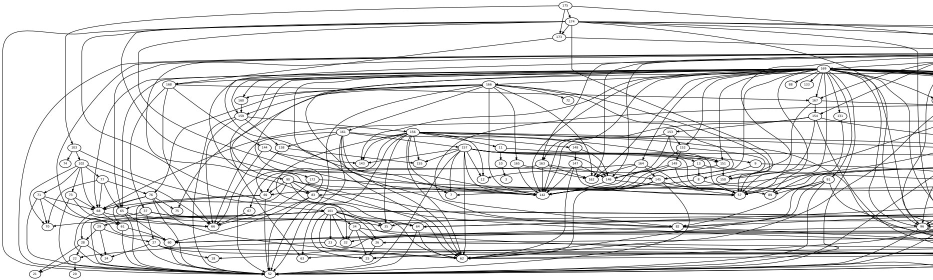
- more 50 pages of mathematical proofs
- very detailed!
- more than 7,000 lines and 220,000 characters
- with dependencies!

Mathematicians at work for Lax-Milgram theorem

- more 50 pages of mathematical proofs
- very detailed!
- more than 7,000 lines and 220,000 characters
- with dependencies!

Mathematicians at work for Lax-Milgram theorem

- more 50 pages of mathematical proofs
- very detailed!
- more than 7,000 lines and 220,000 characters
- with dependencies!



Proof engineering

Let us build upon the Coquelicot library (Boldo, Lelay, Melquiond)

+ general spaces

Proof engineering

Let us build upon the Coquelicot library (Boldo, Lelay, Melquiond)

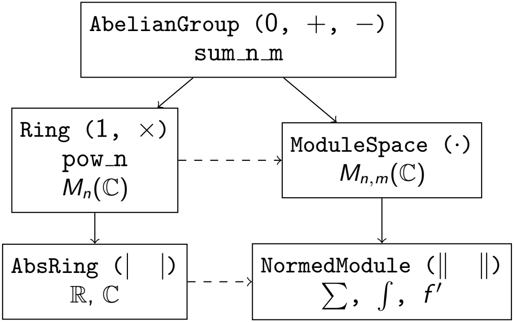
+ general spaces
+ many existing theorems

Proof engineering

Let us build upon the Coquelicot library (Boldo, Lelay, Melquiond)

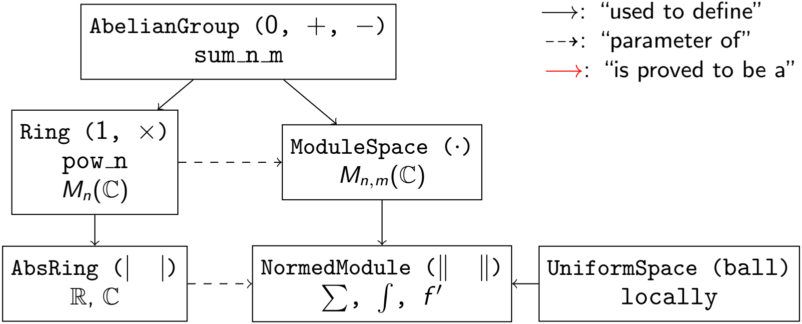
+ general spaces
+ many existing theorems
- not always the space we need

Enriched Hierarchy

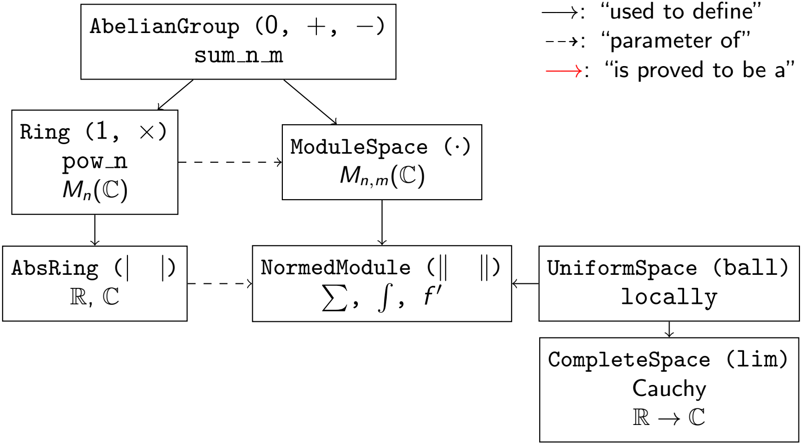


⟶: "used to define"
⇢: "parameter of"
⟶: "is proved to be a"

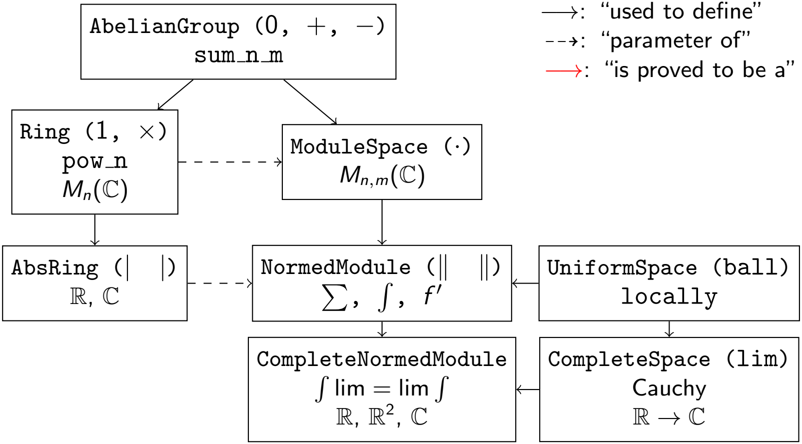
Enriched Hierarchy



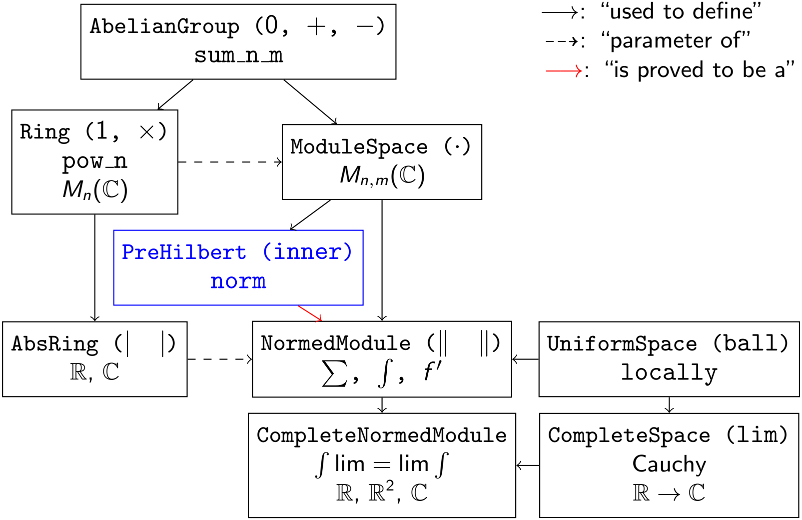
Enriched Hierarchy



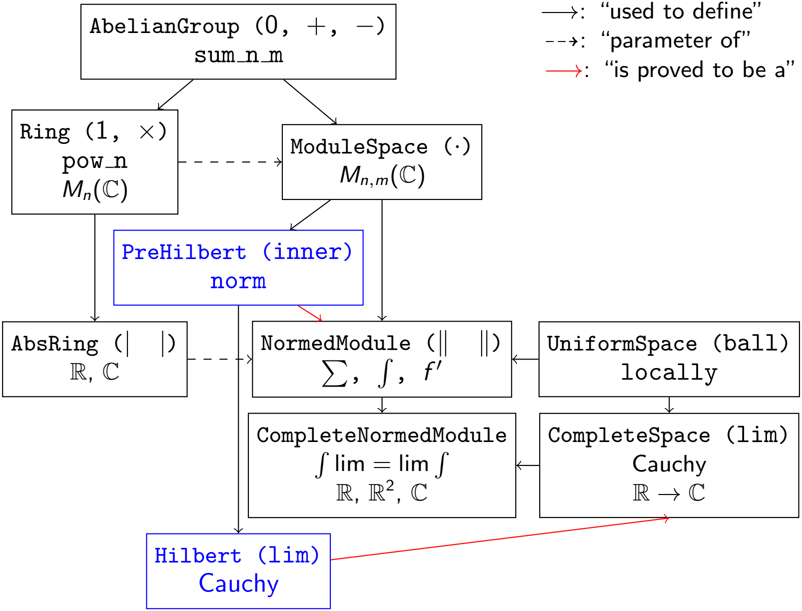
Enriched Hierarchy



Enriched Hierarchy



Enriched Hierarchy



Summary of the work done

- results about functional spaces, linear and bilinear mappings

Summary of the work done

- results about functional spaces, linear and bilinear mappings
- fixed-point theorem in a sub-complete normed module

Summary of the work done

- results about functional spaces, linear and bilinear mappings
- fixed-point theorem in a sub-complete normed module
- decide if a space ($\geq$ NormedModule) is only zero

Summary of the work done

- results about functional spaces, linear and bilinear mappings
- fixed-point theorem in a sub-complete normed module
- decide if a space ($\geq$ NormedModule) is only zero
- norm on functions (`operator_norm`) on $\mathbb{R} \cup \{+\infty\}$

Summary of the work done

- results about functional spaces, linear and bilinear mappings
- fixed-point theorem in a sub-complete normed module
- decide if a space ($\geq$ NormedModule) is only zero
- norm on functions (`operator_norm`) on $\mathbb{R} \cup \{+\infty\}$
- 8 equivalences of continuity of linear mappings

Summary of the work done

- results about functional spaces, linear and bilinear mappings
- fixed-point theorem in a sub-complete normed module
- decide if a space ($\geq$ NormedModule) is only zero
- norm on functions (`operator_norm`) on $\mathbb{R} \cup \{+\infty\}$
- 8 equivalences of continuity of linear mappings
- definitions of pre-Hilbert and Hilbert spaces in Coquelicot hierarchy

Summary of the work done

- results about functional spaces, linear and bilinear mappings
- fixed-point theorem in a sub-complete normed module
- decide if a space ($\geq$ NormedModule) is only zero
- norm on functions (`operator_norm`) on $\mathbb{R} \cup \{+\infty\}$
- 8 equivalences of continuity of linear mappings
- definitions of pre-Hilbert and Hilbert spaces in Coquelicot hierarchy
- define `clm`: the set of the continuous linear mappings

Summary of the work done

- results about functional spaces, linear and bilinear mappings
- fixed-point theorem in a sub-complete normed module
- decide if a space ($\geq$ NormedModule) is only zero
- norm on functions (`operator_norm`) on $\mathbb{R} \cup \{+\infty\}$
- 8 equivalences of continuity of linear mappings
- definitions of pre-Hilbert and Hilbert spaces in Coquelicot hierarchy
- define `clm`: the set of the continuous linear mappings
- prove it is a `NormedModule`, to consider `clm` E (`clm` E $\mathbb{R}$)

Summary of the work done

- results about functional spaces, linear and bilinear mappings
- fixed-point theorem in a sub-complete normed module
- decide if a space ($\geq$ NormedModule) is only zero
- norm on functions (`operator_norm`) on $\mathbb{R} \cup \{+\infty\}$
- 8 equivalences of continuity of linear mappings
- definitions of pre-Hilbert and Hilbert spaces in Coquelicot hierarchy
- define `clm`: the set of the continuous linear mappings
- prove it is a `NormedModule`, to consider `clm` E (`clm` E $\mathbb{R}$)
- prove Lax-Milgram theorem and Céa's lemma

Summary of the work done

- results about functional spaces, linear and bilinear mappings
- fixed-point theorem in a sub-complete normed module
- decide if a space ($\geq$ NormedModule) is only zero
- norm on functions (`operator_norm`) on $\mathbb{R} \cup \{+\infty\}$
- 8 equivalences of continuity of linear mappings
- definitions of pre-Hilbert and Hilbert spaces in Coquelicot hierarchy
- define `clm`: the set of the continuous linear mappings
- prove it is a `NormedModule`, to consider `clm` E (`clm` E $\mathbb{R}$)
- prove Lax-Milgram theorem and Céa's lemma
- for a total of about 10k lines of Coq and 430 lemmas/definitions

Lax-Milgram Theorem and Céa's Lemma

Theorem (Lax-Milgram)

Let E : $\mathtt{Hilbert}$, $f \in E'$, $C, \alpha \in \mathbb{R}_+^*$. Let $\varphi : E \to \mathtt{Prop}$, φ $\mathtt{ModuleSpace}$-compatible and complete. Let a be a bilinear form of E bounded by C and α-coercive. Then:

$$\exists! u \in E, \varphi(u) \wedge \forall v \in E, \varphi(v) \Longrightarrow f(v) = a(u, v) \wedge \|u\|_E \leq \frac{1}{\alpha} |||f|||_\varphi.$$

Lemma (Céa)

Let E : $\mathtt{Hilbert}$, $f \in E'$, $0 < \alpha$. Let $\varphi : E \to \mathtt{Prop}$, φ $\mathtt{ModuleSpace}$-compatible and complete. Let a be a bilinear form of E, bounded by $C > 0$ and α-coercive. Let u and u_φ be the solutions given by Lax–Milgram Theorem respectively on E and on the subspace φ. Then:

$$\forall v_\varphi \in E, \varphi(v_\varphi) \Longrightarrow \|u - u_\varphi\|_E \leq \frac{C}{\alpha} \|u - v_\varphi\|_E .$$

Where are we?

Towards the Coq formalization of the finite element method:

- Lax-Milgram theorem (✓)

Where are we?

Towards the Coq formalization of the finite element method:

- Lax-Milgram theorem (✓)
- requires the subspace to be complete
  (✓ for finite-dimensional subspaces)

Where are we?

Towards the Coq formalization of the finite element method:

- Lax-Milgram theorem (✓)
- requires the subspace to be complete
  (✓ for finite-dimensional subspaces)
- requires E to be a Hilbert space

Where are we?

Towards the Coq formalization of the finite element method:

- Lax-Milgram theorem (✓)
- requires the subspace to be complete
  (✓ for finite-dimensional subspaces)
- requires E to be a Hilbert space
- E will be instantiated as the Sobolev space L_2

Where are we?

Towards the Coq formalization of the finite element method:

- Lax-Milgram theorem (✓)
- requires the subspace to be complete (✓ for finite-dimensional subspaces)
- requires E to be a Hilbert space
- E will be instantiated as the Sobolev space L_2

$\Rightarrow$ prove that L_2 is an Hilbert space

Where are we?

Towards the Coq formalization of the finite element method:

- Lax-Milgram theorem (✓)
- requires the subspace to be complete
  (✓ for finite-dimensional subspaces)
- requires E to be a Hilbert space
- E will be instantiated as the Sobolev space L_2

⇒ prove that L_2 is an Hilbert space

⇒ Lebesgue integration!

Where are we?

Towards the Coq formalization of the finite element method:

- Lax-Milgram theorem (✓)
- requires the subspace to be complete
  (✓ for finite-dimensional subspaces)
- requires E to be a Hilbert space
- E will be instantiated as the Sobolev space L_2

$\Rightarrow$ prove that L_2 is an Hilbert space

$\Rightarrow$ Lebesgue integration!

- ...

Outline

Outline

Measurability

Given a set `E→ Prop`, is it measurable?

Measurability

Given a set `E→ Prop`, is it measurable?

We chose the definition from the generator sets:

```
Context {E : Type}.

(* initialization sets *)
Variable gen : (E → Prop) → Prop.

Inductive measurable : (E→ Prop) → Prop :=
   | measurable_gen : forall omega, gen omega → measurable omega
   | measurable_empty : measurable (fun _ ⇒ False)
   | measurable_compl : forall omega,
        measurable (fun x ⇒ not (omega x)) → measurable omega
   | measurable_union_countable :
    forall omega:nat → (E→ Prop),
      (forall n, measurable (omega n)) →
         measurable (fun x ⇒ exists n, omega n x).
```

The measurable sets are aka σ-algebras.

Measurability

Advantages of `Inductive`:
$\Rightarrow$ induction is possible
$\Rightarrow$ easy theorems

Measurability

Advantages of `Inductive`:
$\Rightarrow$ induction is possible
$\Rightarrow$ easy theorems

We defined generators on $\mathbb{R}$ and $\overline{\mathbb{R}}$:

```
Definition gen_R_cc := (fun om => exists a b, (forall x, om x <-> a <= x <= b)).
Definition gen_Rbar_mc := (fun om => exists a, (forall x, om x <-> Rbar_le a x)).
```

Measurability

Advantages of `Inductive`:
⇒ induction is possible
⇒ easy theorems

We defined generators on $\mathbb{R}$ and $\overline{\mathbb{R}}$:

```
Definition gen_R_cc := (fun om ⇒ exists a b, (forall x, om x ↔ a <= x <= b)).
Definition gen_Rbar_mc := (fun om ⇒ exists a, (forall x, om x ↔ Rbar_le a x)).
```

But we may use other generators and prove the measurable sets are the same. For instance `a` $<$ `x` $<$ `b` or with `a` and `b` in $\mathbb{Q}$.

Measurability

Advantages of `Inductive`:
⇒ induction is possible
⇒ easy theorems

We defined generators on $\mathbb{R}$ and $\overline{\mathbb{R}}$:

```
Definition gen_R_cc := (fun om ⇒ exists a b, (forall x, om x ↔ a <= x <= b)).
Definition gen_Rbar_mc := (fun om ⇒ exists a, (forall x, om x ↔ Rbar_le a x)).
```

But we may use other generators and prove the measurable sets are the same. For instance `a < x < b` or with `a` and `b` in $\mathbb{Q}$.

And we proved that it is equivalent to the usual Borel σ-algebras:

```
Lemma measurable_R_open : forall om,
  measurable gen_R_cc om ↔ measurable open om.
```

Measurable functions

A function $f : E \to F$ is measurable if the set $A(f(x))$ is measurable in F for all measurable sets A in E:

```
Definition measurable_fun : (E → F) → Prop :=
  fun f ⇒ (forall (A: F → Prop), measurable genF A →
  measurable genE (fun x ⇒ A (f x))).
```

Measurable functions

A function $f : E \to F$ is measurable if the set $A(f(x))$ is measurable in F for all measurable sets A in E:

```
Definition measurable_fun : (E → F) → Prop :=
   fun f ⇒ (forall (A: F → Prop), measurable genF A →
   measurable genE (fun x ⇒ A (f x))).
```

The sum and multiplication by a scalar of measurable functions on $\mathbb{R}$ and $\overline{\mathbb{R}}$ are measurable functions.

Measurable functions

A function $f : E \to F$ is measurable if the set $A(f(x))$ is measurable in F for all measurable sets A in E:

```
Definition measurable_fun : (E → F) → Prop :=
   fun f ⇒ (forall (A: F → Prop), measurable genF A →
   measurable genE (fun x ⇒ A (f x))).
```

The sum and multiplication by a scalar of measurable functions on $\mathbb{R}$ and $\overline{\mathbb{R}}$ are measurable functions.

When considering the restriction of f on the subset A.

```
Lemma measurable_fun_when_charac :
  forall (f f':E→ Rbar) (A : E→ Prop),
   measurable gen A →
   (forall x, A x → f x = f' x) →
   measurable_fun_Rbar f' →
   measurable_fun_Rbar (fun x ⇒ Rbar_mult (f x) (charac A x)).
```

with `charac A` the characteristic function $\mathbb{1}_A$.

Outline

Measure definition

We choose to not (yet) define the Lebesgue measure, but define what a measure is supposed to satisfy:

```
Context {E : Type}.
Variable gen : (E → Prop) → Prop.

Record measure := mk_measure {
  meas :> (E→ Prop) → Rbar ;
  meas_False : meas (fun _ ⇒ False) = 0 ;
  meas_ge_0: forall om, Rbar_le 0 (meas om) ;
  meas_sigma_additivity : forall omega :nat → (E→ Prop),
    (forall n, measurable gen (omega n)) →
    (forall n m x, omega n x → omega m x → n = m)
    → meas (fun x ⇒ exists n, omega n x)
          = Sup_seq (fun n ⇒ sum_Rbar n (fun m ⇒ meas (omega m)))
}.
```

Note that we have at least a measure: the Dirac measure.

Measure properties

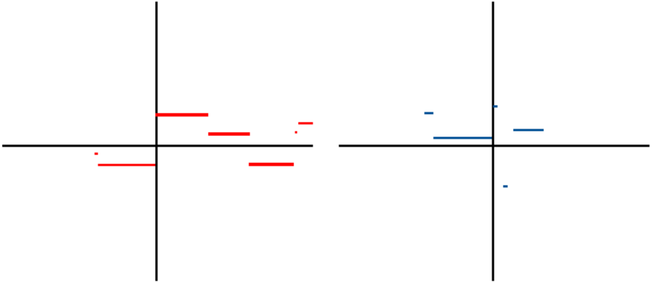
Many properties hold for all measures such as:

```
Lemma measure_Boole_ineq : forall (mu:measure) (A:nat → E→ Prop) (N : nat),
    (forall n, n <= N → measurable gen (A n)) →
      Rbar_le (mu (fun x ⇒ exists n, n <= N ∧ A n x))
              (sum_Rbar N (fun m ⇒ mu (A m))).
```

$$\mu\left(\bigcup_{i\in[0..N]} A_i\right) \leq \sum_{i\in[0..N]} \mu(A_i)$$

Outline

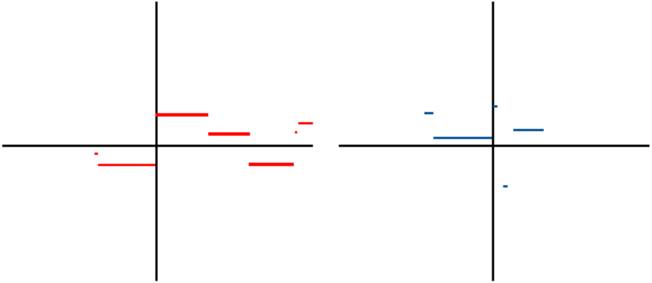
Simple functions?



Examples of simple functions @ mathonline

$$f = \sum_{y \in f(E)} \mathbb{1}_{f^{-1}(\{y\})}$$

Simple functions?



Examples of simple functions @ mathonline

$$f = \sum_{y \in f(E)} \mathbb{1}_{f^{-1}(\{y\})}$$

We have tried various definitions of simple functions, especially as we prefer to sum over a finite set of values.

Simple functions definition

```
Definition finite_vals : (E→ R) → (list R) → Prop :=
    fun f l ⇒ forall y, In (f y) l.
```

⇒ OK, but not unique.

Simple functions definition

```
Definition finite_vals : (E→ R) → (list R) → Prop :=
    fun f l ⇒ forall y, In (f y) l.
```

⇒ OK, but not unique.

```
Definition finite_vals_canonic : (E→ R) → (list R) → Prop :=
   fun f l ⇒ (LocallySorted Rlt l) ∧
             (forall x, In x l → exists y, f y = x) ∧
             (forall y, In (f y) l).
```

⇒ unique!

We were able to construct the second list from the first.

Simple functions integration

$$\int f \, d\mu \stackrel{\text{def.}}{=} \sum_{a \in f(X)} a \, \mu\left(f^{-1}(a)\right) \quad \in \overline{\mathbb{R}}$$

Simple functions integration

$$\int f \, d\mu \stackrel{\text{def.}}{=} \sum_{a \in f(X)} a \, \mu \left(f^{-1}(a) \right) \quad \in \overline{\mathbb{R}}$$

```
Definition SF_aux : (E→ R) → (list R) → Prop :=
  fun f l ⇒ finite_vals_canonic f l ∧
    (forall a, measurable gen (fun x ⇒ f x = a)).

Definition SF : (E→ R) → Set := fun f ⇒ { l | SF_aux f l}.

Definition af1 (f:E→ R) :=
  (fun a :  Rbar ⇒ Rbar_mult a (mu (fun (x:E) ⇒ f x = a))).

Definition LInt_simple_fun_p :=
   fun (f:E→ R) (H:SF gen f) ⇒ let l:= (proj1_sig H) in
     sum_Rbar_map l (af1 f).
```

We proved the value does not depends on the proof `H`.

Simple functions integration

$$\int f \, d\mu \stackrel{\text{def.}}{=} \sum_{a \in f(X)} a \, \mu\left(f^{-1}(a)\right) \quad \in \overline{\mathbb{R}}$$

```
Definition SF_aux : (E→ R) → (list R) → Prop :=
  fun f l ⇒ finite_vals_canonic f l ∧
    (forall a, measurable gen (fun x ⇒ f x = a)).

Definition SF : (E→ R) → Set := fun f ⇒ { l | SF_aux f l}.

Definition af1 (f:E→ R) :=
  (fun a :  Rbar ⇒ Rbar_mult a (mu (fun (x:E) ⇒ f x = a))).

Definition LInt_simple_fun_p :=
   fun (f:E→ R) (H:SF gen f) ⇒ let l:= (proj1_sig H) in
     sum_Rbar_map l (af1 f).
```

We proved the value does not depends on the proof `H`.

⇒ theorems about sum, multiplication by a scalar and change of variable

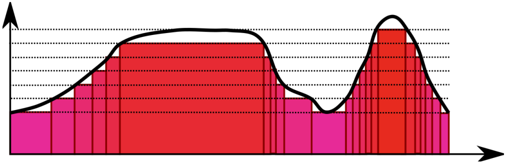
Outline

Lebesgue integral

$$\int f \, d\mu \stackrel{\text{def.}}{=} \sup_{\varphi \in \mathcal{SF}_+, \varphi \leq f} \int \varphi \, d\mu \quad \in \overline{\mathbb{R}}$$

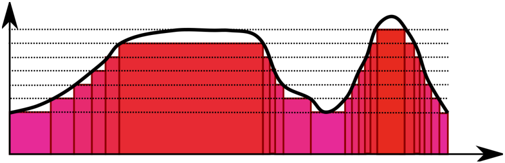
Lebesgue integral

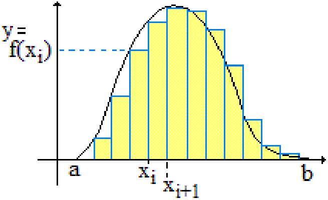
$$\int f \, d\mu \overset{\text{def.}}{=} \sup_{\varphi \in \mathcal{SF}_+, \varphi \leq f} \int \varphi \, d\mu \quad \in \overline{\mathbb{R}}$$



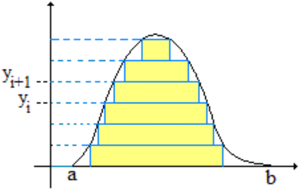
Lebesgue integral

$$\int f \, d\mu \stackrel{\text{def.}}{=} \sup_{\varphi \in \mathcal{SF}_+, \varphi \leq f} \int \varphi \, d\mu \quad \in \overline{\mathbb{R}}$$





Riemann integral *vs*



Lebesgue integral

© Serge Mehl chronomath.com

Lebesgue integral definition

$$\int f \, d\mu \stackrel{\text{def.}}{=} \sup_{\varphi \in \mathcal{SF}_+, \varphi \leq f} \int \varphi \, d\mu \quad \in \overline{\mathbb{R}}$$

```
Definition LInt_p :(E→ Rbar) → Rbar := fun f ⇒
     Rbar_lub (fun x ⇒ exists (g:E→ R), exists (Hg: SF gen g),
                        non_neg g ∧
                        (forall (z:E), Rbar_le (g z) (f z)) ∧
                        LInt_simple_fun_p mu g Hg = x).
```

Theorems (1/3)

Theorem (Beppo Levi, monotone convergence)

Let $(f_n)_{n\in\mathbb{N}}$ be a sequence of nonnegative measurable functions, that is pointwise nondecreasing. Then, the pointwise limit of $(f_n)_{n\in\mathbb{N}}$ is nonnegative and measurable, and we have in $\overline{\mathbb{R}}$

$$\int \lim_{n\to\infty} f_n \, d\mu = \lim_{n\to\infty} \int f_n \, d\mu.$$

Theorems (2/3)

Theorem (Fatou–Lebesgue)

Let $(f_n)_{n\in\mathbb{N}}$ be a sequence of nonnegative measurable functions. Then, we have in $\overline{\mathbb{R}}$

$$\int \liminf_{n\to\infty} f_n \, d\mu \leq \liminf_{n\to\infty} \int f_n \, d\mu.$$

```
Theorem Fatou_Lebesgue : forall f: nat → E → Rbar,
    (forall n, non_neg (f n)) →
    (forall n, measurable_fun_Rbar gen (f n)) →
    Rbar_le (LInt_p mu (fun x ⇒ LimInf_seq' (fun n ⇒ f n x)))
            (LimInf_seq' (fun n ⇒ LInt_p mu (f n))).
```

Theorems (3/3): focus on a hard one

Theorems (3/3): focus on a hard one

$$\int (f+g) = \int f + \int g$$

```
Lemma LInt_p_plus : forall f g,
    non_neg f → non_neg g →
    measurable_fun_Rbar gen f → measurable_fun_Rbar gen g →
    LInt_p mu (fun x ⇒ Rbar_plus (f x) (g x))
        = Rbar_plus (LInt_p mu f) (LInt_p mu g).
```

Proof of $\int(f+g) = \int f + \int g$ (1/2)

It needs adapted sequences:

```
Definition is_adapted_seq (f:E→ Rbar) (phi:nat→ E→ R) :=
    (forall n, non_neg (phi n)) ∧
    (forall (x:E) n, phi n x <= phi (S n) x) ∧
    (forall n, exists l, SF_aux gen (phi n) l) ∧
    (forall (x:E), is_sup_seq (fun n ⇒ phi n x) (f x)).
```

as their limit gives the integral:

```
Lemma LInt_p_with_adapted_seq :
   forall f phi, is_adapted_seq f phi →
      is_sup_seq (fun n ⇒ LInt_p mu (phi n)) (LInt_p mu f).
```

Proof of $\int(f+g) = \int f + \int g$ (2/2)

Adapted sequences may be defined like that:

$$\forall x, \quad f_n(x) \stackrel{\text{def.}}{=} \begin{cases} \dfrac{\lfloor 2^n f(x) \rfloor}{2^n} & \text{when } f(x) < n, \\ n & \text{otherwise.} \end{cases}$$

Proof of $\int(f+g) = \int f + \int g$ (2/2)

Adapted sequences may be defined like that:

$$\forall x, \quad f_n(x) \stackrel{\text{def.}}{=} \begin{cases} \dfrac{\lfloor 2^n f(x) \rfloor}{2^n} & \text{when } f(x) < n, \\ n & \text{otherwise.} \end{cases}$$

that may be written in Coq as:

```
Definition mk_adapted_seq (n:nat) (x:E) :=
  match (Rbar_le_lt_dec (INR n) (f x)) with
          | left _ ⇒ INR n
          | right _ ⇒ round radix2 (FIX_exp (−n)) Zfloor (f x)
  end.
```

relying on fixed-point arithmetic defined by the Flocq library!!

And then:

```
Lemma mk_adapted_seq_is_adapted_seq :
   is_adapted_seq f mk_adapted_seq.
```

Outline

Conclusion

For the Lebesgue integration:

- mathematicians at work: 184 pages and 600 lemmas/definitions
- formal proofs at work: 11 k lines lines and 635 lemmas/definitions

Conclusion

For the Lebesgue integration:

- mathematicians at work: 184 pages and 600 lemmas/definitions
- formal proofs at work: 11 k lines lines and 635 lemmas/definitions

Difficult parts:

- handling subspaces (mainly with $\mathbb{1}$ here)
- having usable simple functions

Perspectives

- extend to functions of varying sign

$$\int f = \int \max(0, f) - \int \max(0, -f)$$

Perspectives

- extend to functions of varying sign

$$\int f = \int \max(0, f) - \int \max(0, -f)$$

- define the Lebesgue measure

Perspectives

- extend to functions of varying sign

$$\int f = \int \max(0, f) - \int \max(0, -f)$$

- define the Lebesgue measure
- merge/take advantage of mathcomp-analysis

Perspectives

- extend to functions of varying sign

$$\int f = \int \max(0, f) - \int \max(0, -f)$$

- define the Lebesgue measure
- merge/take advantage of mathcomp-analysis
- write the corresponding article

Perspectives

- extend to functions of varying sign

$$\int f = \int \max(0, f) - \int \max(0, -f)$$

- define the Lebesgue measure
- merge/take advantage of mathcomp-analysis
- write the corresponding article
- define L_2 and prove it is a Hilbert

Perspectives

- extend to functions of varying sign

$$\int f = \int \max(0, f) - \int \max(0, -f)$$

- define the Lebesgue measure
- merge/take advantage of mathcomp-analysis
- write the corresponding article

- define L_2 and prove it is a Hilbert
- define the FEM algorithm and prove it

Perspectives

- extend to functions of varying sign

$$\int f = \int \max(0, f) - \int \max(0, -f)$$

- define the Lebesgue measure
- merge/take advantage of mathcomp-analysis
- write the corresponding article

- define L_2 and prove it is a Hilbert
- define the FEM algorithm and prove it
- prove a real implementation (in floating-point arithmetic)

Thank you for your attention