Réunion LiberAbaci
Inria Paris

La bibliothèque coq-num-analysis

Sylvie Boldo *et al.*

Inria, Université Paris-Saclay

20 septembre 2022

Motivations

$\mathfrak{Mathematics}$

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

Motivations

$\mathfrak{Mathematics}$

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

Applied Mathematics

numerical scheme, convergence
algorithms + theorems

Motivations

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 + ?

Motivations

Mathem

Applied N

Computer

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

theorems

PARANOIA

me, convergence

entation

programs

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)

$\Rightarrow$ real program implementing the scheme/method

Let us machine-check this kind of programs!

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...

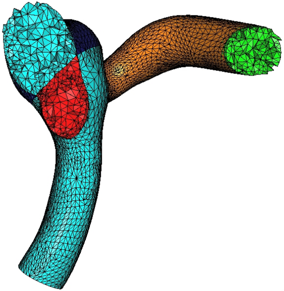
The conclusion of the investigation was that the loss was caused by a failure in a cell wall, resulting in a serious crack and a leakage that the pumps were not able to cope with. The wall failed as a result of a combination of a serious error in the finite element analysis and insufficient anchorage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

The Finite Element Method (FEM) is one of 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 (XLiFE++) implementing the FEM

@ V. Martin

Who? What?

Authors:

- Sylvie Boldo,
- François Clément,
- Florian Faissole,
- Vincent Martin,
- Micaela Mayero,
- Houda Mouhcine.

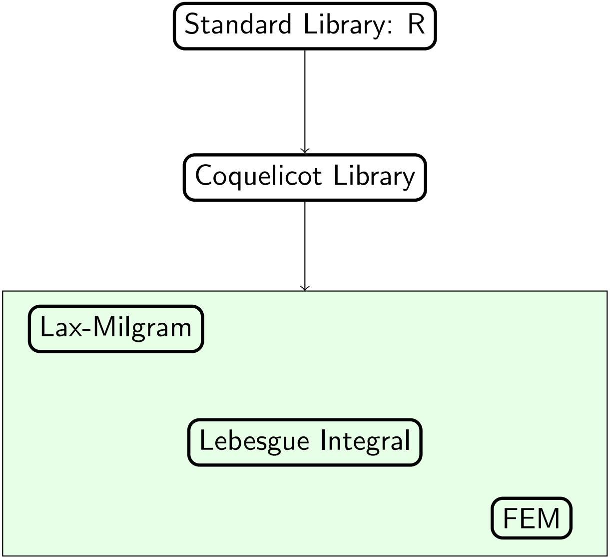
Goal:

- support for numerical analysis in Coq
- notably for finite elements

Relies on pen & paper proofs: RR-8934 and RR-9386

- *The Lax-Milgram Theorem. A detailed proof to be formalized in Coq*
- *Lebesgue integration. Detailed proofs to be formalized in Coq*

High-level description



Example of a Theorem

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))).
```

About the library

coq-num-analysis

- git: `https://lipn.univ-paris13.fr/coq-num-analysis/tree/master/`
- **opam**: coq-num-analysis

Contains

- Lax-Milgram: CPP'17 – 13 files – 11,000 loC – 350 lemmas
- Lebesgue integral: JAR'22 – 46 files – 29,000 loC – 2,640 lemmas
- Bochner integral: 15 files – 7,000 loC – 200 lemmas
- Finite Element Method: WIP, will rely on math-comp

What about LiberAbaci?

- vanilla Coq
- more down-to-earth (few implicits): easy to get into
- parts to be taken: Lebesgue integral?
- library to be cleaned