Présentation du module Initiation aux preuves formelles

Marie Kerjean, Micaela Mayero, Pierre Rousselin

Inria Paris
20 septembre 2022

Contexte

Contenu

Impressions, retours

Contexte

Contenu

Impressions, retours

Public

- Université Paris 13, campus de Villetaneuse
- L1 double-licence maths/info, premier semestre
- 2 groupes de 25

Génèse

- PRAG depuis septembre 2020 au département d'informatique
- Avant, thèse de mathématiques au LAGA (univ. Paris 13)
- Responsabilité double-licence maths-info en 2021
- Constat : en L1 DL aucune différence avec la L1 info
- Idée de créer un « module d'accueil » vraiment maths et info pour cette promotion DL
- Évidemment... (presque) sans moyen supplémentaire.
- Remplacer Méthodologie du Travail Universitaire (18h).
- Apprentissage de la rigueur, indispensable en maths et en info
- Et évidemment le côté ludique, donner aux étudiants l'envie de chercher des preuves

Labos

- Laboratoires de maths (LAGA) et d'informatique (LIPN) très proches
- Groupe de recherche de Micaela Mayero (LIPN) sur la formalisation de l'intégrale de Lebesgue en coq
- Arrivée de Marie Kerjean (analyse fonctionnelle avec coq + math-comp-analysis) comme chargée de recherche au LIPN en 2020
- Donc, dès l'entrée en L1, cours adossé à la recherche, bienvenue à l'université.

Préparations, discussions avec l'ancien responsable DL

- Peur de créer des confusions de notations.
- `A -> B` (A implique B) et `f : E -> F` (fonction de E vers F).
- Pas d'ensembles, `E -> Prop` au lieu de $\mathcal{P}(E)$
- Pas de table de vérité, ... des différences significatives avec le cours d'introduction aux mathématiques.

Préparations, discussions avec l'ancien responsable DL

- Peur de créer des confusions de notations.
- `A -> B` (A implique B) et `f : E -> F` (fonction de E vers F).
- Pas d'ensembles, `E -> Prop` au lieu de $\mathcal{P}(E)$
- Pas de table de vérité, ... des différences significatives avec le cours d'introduction aux mathématiques.

Finalement, nous avons ignoré ces craintes : les étudiants de maths-info doivent pouvoir changer de syntaxe selon le contexte.

Contexte

Contenu

Impressions, retours

Attention

- Nous avons dû faire certains choix.
- Il est certain que ce ne sont pas les seuls possibles, et probable qu'ils ne soient pas les meilleurs.
- On ne cherche pas à dire « il faut faire comme ça », mais plutôt « on a fait comme ça » et expliquer (quand c'est possible) « pourquoi on a décidé de faire comme ça. »

Choix et préparation du module

- Séances *hands-on* en TP et c'est tout
- Influence très importante de *Software foundations* de Pierce et al
- Vanilla coq
- Comme dans *Software Foundations*, fichiers `.v` autonomes avec le « cours » en commentaires et les preuves à remplir.
- Éventuellement dans un navigateur pour une meilleure mise en forme (avec `coqdoc`)
- Sujets souvent prêts la veille (voire le jour même !) des séances

Choix (2)

- Ne rien « mettre sous le tapis » : logique intuitionniste, associativité à droite de `->`, ...
- Les étudiants passionnés devraient pouvoir écrire leurs propres théorèmes (voire leurs propres définitions) et les prouver (autonomie).
- Côté « maths-info » assumé, c'est ok de parler de types, de fichiers source, etc (pas de jscoq, différence avec deaduction et edukera).
- Pas de propositions inductives à ce niveau.

Idée de départ

- Au départ, idée d'aller jusqu'aux limites de suite.
- Pré-requis : entiers naturels et réels (et bien sûr, logique).

Organisation du cours

- Logique propositionnelle intuitionniste
- Entiers naturels et induction
- (Petite évaluation)
- Quantificateurs et un peu de calcul des prédicats/ensembles à la coq
- Réels : point de vue axiomatique (en fait corps ordonné)
- Analyse (suites réelles)
- + devoir à la maison (trop dur)
- + TP noté final d'1h

Logique1.v

```
Theorem imp_refl : forall P : Prop, P → P.
Proof.
  (* Soit P une proposition quelconque. *)
  intros P.
  (* Pour montrer une implication on suppose que ce qui est à gauche est prouvé.
     On doit prouver ce qui est à droite avec cette hypothèse supplémentaire. *)
  (* On suppose (hypothèse (HP)) que P est prouvée. *)
  intros HP.
  (* On doit prouver P. Mais cela fait partie des hypothèses ! *)
  assumption.
Qed. (* Quod erat demonstrandum. Ce qu'il fallait démontrer. *)

(** **** Exercice : Prouver le théorème suivant. *)
Theorem imp_ex1 : forall P Q : Prop, P → (Q → P).
Proof.
  (* Début Solution *)
  (* Soient P et Q deux propositions quelconques. *)
  intros P Q.
  (* Supposons (hypothèse (HP)) que P est prouvée. *)
  intros HP.
  (* Supposons (hypothèse (HQ)) que Q est prouvée. *)
  intros HQ.
  (* Il reste à prouver P, or P est prouvée par hypothèse. *)
  assumption.
Qed.
  (* Fin Solution *)
```

Logique1.v

- On suit la méthode de *Logical Foundations* : exemple(s) à suivre dans coq, lien avec les mathématiques connues, puis exercices sous la forme de preuves à remplir.
- Raisonnements vers l'arrière et vers l'avant (avec `apply in`).
- Négation, `unfold not`, `False`, `destruct`, `exfalso` : un gros morceau à digérer dès le début.
- Conjonction, `destruct` et `split` : élimination et introduction.
- Disjonction, `destruct` et `left`/`right` : élimination et introduction.
- En fin de sujet, logique classique.

Naturels.v

- Présentation de `nat` comme type inductif, tactique `discriminate`
- Tactiques `simpl` et `reflexivity`
- Tactiques `induction` et `rewrite`
- Tactique `destruct` pour les preuves par cas.
- Jusqu'à la preuve de `mul_commutative`.
- Difficulté principale : instancier (partiellement) les théorèmes pour aider coq à unifier.

L'ordre perdu

- On ne veut pas parler de `bool` : c'est déjà dur de comprendre la logique de coq, alors comprendre une logique définie dans la logique de coq...
- Pas de proposition inductive.
- Donc pas d'ordre sur $\mathbb{N}$... (ou alors en cachant sa définition, ce qu'on n'a pas voulu faire).

Calcul des prédicats et « ensembles »

- Exemple de chose qu'on aimerait faire comprendre :

```
(** Est-ce que vous savez expliquer pourquoi l'implication inverse
    n'est pas vrai ?  Vous pouvez éventuellement essayer de la prouver
    ci-dessous et de voir où vous êtes bloqués. *)
Lemma forall_p_or_q_false :
  forall x, (P x \/ Q x) → (forall x : X, P x) \/ (forall y : X, Q y).
Proof.
Abort.
```

- Quantificateur existentiel, introduction (`exists`) et élimination (`destruct`).
- « Ensembles », en fait `A -> Prop`.
- Composition des fonctions, injections, surjections, bijections.

CorpsOrdonné.v

- Le corps des réels est présenté de façon axiomatique.
- Les axiomes sont introduits petit à petit, avec des exercices pour les manipuler.

```
Check Rplus_comm. (* commutativité, AXIOME 1 *)
Check Rplus_assoc. (* associativité, AXIOME 2 *)
Check Rplus_0_l. (* 0 est élément neutre à gauche, AXIOME 3 *)
Check Rplus_0_r. (* 0 est élément neutre à droite, THÉORÈME (qui se déduit
  facilement de la commutativité et de Rplus_0_l *)

Theorem oppose_unique : forall x y z : R, x + y = 0 /\ x + z = 0 → y = z.
Proof.
  (* ... *)
Qed.
```

CorpsOrdonné.v

- Plus de `simpl` possible, seulement `rewrite`, avec les difficultés associées (aider coq à unifier).
- Manipulation de l'ordre. Difficulté :

```
total_order_T
     : forall r1 r2 : R, {r1 < r2} + {r1 = r2} + {r2 < r1}
```

- `Theorem Rlt_0_1: 0 < 1.`
- `Theorem Rinv_0_lt_compat : forall r : R, 0 < r → 0 < / r.`

Suites.v

- On commence par les propriétés de la valeur absolue.
- À partir de là, `lra` est autorisé.
- Premier théorème d'analyse :

```
Lemma small_zero: forall x,
  (forall eps, eps > 0 -> (Rabs x) < eps) -> x = 0.
```

- L'exemple donné est celui de l'unicité de la limite :

```
Theorem UL_sequence:
  forall (Un : nat → R) (l1 l2 : R), Un_cv Un l1 → Un_cv Un l2 → l1 = l2.
Proof.
  unfold Un_cv.
  intros Un l1 l2 Hl1 Hl2.
  (* On va montrer que la distance entre l1 et l2 est aussi petite qu'on ve
  apply small_dist_equal.
  (* Soit eps > 0. *)
  intros eps Heps.
  (* ... *)
  (* Soit n3 = max(n1, n2). *)
  pose (n3 := (max n1 n2)).
  (* Alors, |Un3 - l1| < eps / 2 *)
  assert (Hdistl1: R_dist (Un n3) l1 < eps / 2).
  (* ... *)
Qed.
```

- `pose` (ou `set` ...) : est-ce qu'il y a un moyen de nommer l'égalité ?
- Difficultés à comprendre/utiliser la bibliothèque standard sur les réels.

Contexte

Contenu

Impressions, retours

À la fin

- La partie logique propositionnelle est plutôt bien, voire très bien comprise (la corrélation est forte entre « mal comprendre la logique propositionnelle » et « rater sa L1 »).
- Presque tous les étudiants savent prouver des égalités simples par induction.
- Les ennuis apparaissent avec le calcul des prédicats (partie donc à retravailler ou édulcorer).
- La partie avec les réécritures dans $\mathbb{R}$ s'est plutôt bien passée, mais les étudiants ont tout de même accueilli `lra` avec des chants.
- Presque aucun étudiant n'est arrivé à prouver de théorème significatif sur les suites (peut-être trop ambitieux pour 18h au premier semestre). Les difficultés sont aussi mathématiques (la définition de limite n'a-t-elle qu'un rôle cosmétique dans le cours d'analyse au premier semestre de L1 ?)

À la fin (2)

- Ce module a bien renforcé la cohésion du groupe.
- C'est en train de devenir la signature de la double-licence maths-infos, les DL2 de cette année ont déjà prévenu les DL1 qu'ils allaient en ***** avec les preuves formelles.
- Beaucoup de très belles réussites à la fin de la L1.
- Très peu de départs à la fin de la L1.
- Article à paraître dans la gazette de la SMF sur l'usage des assistants de preuve dans l'enseignement des mathématiques à l'université.
- Pour nous, encore beaucoup de travail pour faire mieux !

Un étudiant, dans son devoir à la maison

```
(*
  Petit message :D :

  Votre DM, est d'une difficulté !!! Parmis tout ceux qui sont dans le groupe
  Discord qu'on a créé pour se coordonner, on est, si je ne me trompe pas que
  ~5 à avoir à peine réussi à faire la moitié des exos seulement :P !

  Et perso j'ai commencé le Mardi pendant les vacances ^_^' !

  C'était juste pour vous dire : Courage, vous allez voir des horreurs.

  Sérieusement, je trouve Coq très intéressant, et y a de très fortes chances
  que j'y retourne après que tout ça soit finit. Mais, je trouve que ça aurait
  mérité plus d'heures ou plus d'explications, parce qu'avec les injections et
  sur les suites dans la Partie 4, on se retrouve un peu perdu...

  La pente de difficulté était beaucoup trop raide, et la plupart se sont
  retrouvé perdu (sans même parler de ce DM, où là, tout le monde est perdu !).

  C'est aussi un peu dommage de faire tout ça pour ne plus jamais en faire.
*)
```