

Candidature pour la création d'un laboratoire junior

Projet COQTAIL

Date : de septembre 2010 à septembre 2011

1 Présentation du projet COQTAIL

1.1 Conjoncture

La correspondance de Curry-Howard établit le lien entre une preuve et un processus calculatoire : démontrer un théorème et construire une fonction qui, à partir des hypothèses, *renvoie* la conclusion sont un seul et même problème.

Coq [L:BC04] est un assistant de preuves formelles par ordinateur utilisant cette correspondance dans un sens comme dans l'autre. Il est ainsi possible :

- d'énoncer des théorèmes mathématiques et de les prouver ;
- de définir des spécifications et de fournir une fonction les vérifiant.

Coq permet une construction interactive des preuves ainsi que la définition de tactiques permettant la résolution (totale ou partielle) de buts de manière automatique. Sa puissance n'est plus à démontrer étant donné qu'il a permis la formalisation de la preuve du théorème des quatre couleurs [Gonthier07] ainsi que la création d'un compilateur certifié pour un important sous-ensemble de C [compcert].

1.2 Héritage de COQUILLE

Le projet COQTAIL (Coq Theorems, Abstractions and Implementations, Licence-level) s'est, jusqu'à présent, attaché à fournir des outils (formalisations d'objets et résultats théoriques attachés) permettant d'aborder simplement des problèmes de niveau Licence en Coq. Il fait suite à COQUILLE développé au sein du module Projet Intégré du M1 d'Informatique Fondamentale.

Le travail fourni jusqu'à présent a déjà permis de poser des bases solides au sein de divers domaines (suites réelles, complexes, analyse complexe, séries entières, etc.) et de démontrer des résultats connus ou élégants (formule de Stirling, indénombrabilité de \mathbb{R} , problème de Bâle) faisant l'objet d'une compétition entre les différents assistants de preuve [Freek].

2 Objectifs

Notre objectif est maintenant de mettre à profit les outils développés et la maturité acquise pour aborder des sujets plus fondamentaux et plus complexes. Dans ce cadre, nos efforts seront orientés vers la formalisation et l'étude des équations différentielles d'une part et des graphes d'autre part. Ces formalisations seront, bien entendu, accompagnées des outils nécessaires à leur manipulation, de leurs propriétés les plus basiques et de théorèmes plus ardues (notamment les théorèmes de résolution d'équations différentielles).

Ces deux sujets sont fondamentaux : les équations différentielles sont présentes dans tous les systèmes physiques et si l'on désire modéliser ces systèmes, il sera absolument nécessaire d'être

capable de les manipuler. Notre démarche étant de démontrer les théorèmes de manière la plus constructive possible, il sera possible d'extraire des méthodes d'approximation de nos résultats.

Les graphes sont, quant à eux, très présents en informatique que ce soit pour des problèmes d'ordonnancement, de routage ou en théorie de la complexité. Être capable de les manipuler et de décider l'équivalence de deux graphes permettra donc d'avoir des outils de base pour aborder de tels problèmes.

2.1 Refonder les réels

Il existe actuellement deux grandes formalisations des réels en Coq. D'un côté, la construction des réels en C-Corn [**C-Corn**], et de l'autre, la bibliothèque standard de Coq. C-Corn est une bibliothèque qui permet de calculer avec les réels mais dans laquelle certains énoncés sont indémontrables car elle refuse les propositions non-constructives. À l'inverse, dans la bibliothèque standard, l'axiomatique a été choisie de manière à pouvoir exprimer des propriétés classiques. Malheureusement, ce choix implique l'existence de fonctions non-calculables.

Nous proposons notre propre formalisation des réels qui nous permettra de calculer avec des réels tout en conservant la possibilité de prouver des théorèmes classiques. Cette construction servira de base aux développements d'analyse réelle mais elle sera également reliée à l'axiomatique de la bibliothèque standard afin de faire en sorte que nos résultats soient réutilisables par le plus grand nombre.

2.2 Équations différentielles

Notre principal souci est la formalisation des équations différentielles. Nous allons, bien entendu, aborder les théorèmes de résolution et d'unicité de la solution si les conditions initiales sont fixées. Nous explorerons également des sujets très proches comme les classes de fonctions et les fonctions analytiques.

Les équations différentielles faisant intervenir des dérivées n -ièmes, il paraît légitime de s'inquiéter de l'existence d'une formalisation aisément manipulable de la théorie de l'intégration et des principaux résultats. La première *release* de COQTAIL fournit déjà un ensemble de bibliothèques qui forment une surcouche à la bibliothèque standard permettant une utilisation plus simple de celle-ci.

2.3 Graphes

Les graphes ne disposant pas, à ce jour, de bibliothèques de théorèmes de base et de tactiques simples d'utilisation pour décider de propriétés telles que l'homomorphisme de graphes, ou autres résultats dont on aimerait disposer pour faciliter les preuves de théorèmes plus complexes, nous avons l'intention de concevoir et implémenter une telle bibliothèque. L'enjeu sera de choisir les bonnes définitions, et d'identifier les théorèmes essentiels, de manière à la rendre aussi puissante et simple d'utilisation que possible.

3 Déroulement

Nos méthodes de travail sont directement héritées des mois passés à travailler sur les projets COQUILLE puis COQTAIL. Une phase de bibliographie et de recherche de preuves simples (et con-

structives) précède toute décision. Le choix des structures de données est ensuite fait de manière à trouver un compromis acceptable entre les définitions traditionnelles et les définitions les plus simples à manipuler ; c'est une étape cruciale qui peut faire varier de manière non négligeable la difficulté des preuves à écrire par la suite. Le travail de réécriture des preuves et d'implémentation peut ensuite être découpé suivant les affinités de chacun pour les sujets abordés : l'exercice se prête particulièrement bien au travail en parallèle comme nous l'ont prouvé les six mois passés.

3.1 Quels outils ?

Le projet COQTAIL dispose déjà d'un site internet [**coqtail**] et d'un système de gestion de version de fichiers qui permet le travail collaboratif en parallèle. Nous comptons continuer à utiliser ce mode de fonctionnement dans la mesure où il s'agit d'une des bases du génie logiciel.

3.2 Équipe

L'équipe comporte 6 membres :

- Marc Lasson¹ – doctorant, responsable du laboratoire junior
- Guillaume Allais – normalien
- Marthe Bonamy – normalienne
- Sylvain Dailler – auditeur
- Jean-Marie Madiot – normalien
- Pierre-Marie Pédro – normalien

4 Calendrier et budget

4.1 Calendrier

Le projet débutera en septembre 2010 pour une durée d'un an. Nous prévoyons de publier plusieurs versions qui nous permettront de juger de l'état d'avancement du projet :

- première version fin février 2011
- deuxième version mars-avril 2011 avec une participation au Coq Workshop
- rapport et version finale fin août 2011

4.2 Budget

4.2.1 Groupes de travail

Nous comptons assister à quelques groupes de travail au cours de l'année (à Lyon comme ailleurs) afin de présenter nos résultats à d'autres équipes et échanger des idées à ce sujet.

En comptant l'aller-retour Lyon-Paris à 75 € et la participation à un groupe de travail par personne en moyenne (le déplacement de toute l'équipe n'est pas requis pour chaque présentation), cela nous reviendrait à **450 €** pour l'année soit environ 3 à 6 participations (1 à 2 membres de l'équipe).

1. Courrier électronique : prénom.nom@ens-lyon.fr. Téléphone : (+33)4 72 72 85 82. Adresse : Équipe Plume Laboratoire de l'Informatique du Parallélisme (LIP) ENS Lyon 46, allée d'Italie 69364 Lyon cedex 07

4.2.2 Conférences

Nous prévoyons d'assister aux conférences ITP (*Interactive Theorem Proving*) et au Coq Workshop si ces deux événements sont regroupés comme c'est le cas cette année.²

ITP est une conférence internationale sur la preuve interactive de théorèmes dédiée aux applications et études de cas mais également aux fondements théoriques de la preuve interactive et aux langages de preuves. Ce sera l'occasion pour nous de voir ce qui se fait à l'heure actuelle pour, éventuellement, en tirer de nouveaux objectifs. Le Coq Workshop est l'occasion de proposer des présentations plus informelles et de partager entre développeurs, contributeurs et utilisateurs de Coq. Nous proposerons une présentation du projet COQTAIL et des résultats obtenus afin d'inciter d'autres chercheurs à les réutiliser et à les intégrer dans les contributions, voire la bibliothèque standard si cela est possible.

Nous déposerons des dossiers afin d'obtenir le financement d'une partie de nos frais par la conférence : une centaine de bourses (*student travel support*) sont décernées afin de permettre à des étudiants de venir assister aux conférences (financement jusqu'à **750 €** par personne uniquement sur les frais de transport et de logement).

Cela nous coûterait donc (frais d'inscription seulement) :

- Coq Workshop (42 € par personne)
- ITP (150 € par personne)

Ce qui représente **1152 €** (6×192 €).

4.2.3 Total

Cela fait un budget total de **1600 €**.

2. <http://www.floc-conference.org/ITP-home.html>