Proposition de stage Master 2 Recherche
Preuve interactive d'algorithmes probabilistes

29 novembre 2011

1 Informations générales

Responsable : P. Castéran et A. Zemmari
lieu : LaBRI
e-mail : {casteran,zemmari}@labri.fr
équipes :
Méthodes Formelles, thème : Logiques, Graphes et Langages,
Combinatoire et algorithmes, thème : Algorithmique distribuée.

Mots-clés : Algorithmes probabilistes, Assistant de preuve Coq.

2 Description du sujet

Un algorithme probabiliste est un algorithme qui utilise des tirages de type pile ou face ou des générateurs de nombres aléatoires. À la différence des algorithmes déterministes, le hasard joue un rôle fondamental dans l'exécution de tels algorithmes.

Les algorithmes probabilistes permettent de fournir des solutions parfois plus "efficaces" que les solutions déterministes, ou encore des solutions pour des problèmes qui n'admettent pas de solution déterministe.

Quand on conçoit un algorithme probabiliste pour résoudre un problème, on s'intéresse à sa complexité C et à la probabilité p que l'algorithme résout effectivement ce problème.

Prouver la correction d'un algorithme est un problème récurrent de l'informatique. Certifier que la preuve est correcte est d'autant plus délicat que la preuve est complexe. Pour résoudre ce type de problème, il existe des assistants de preuves tels que **Coq**, **Isabelle** et **HOL** permettant de formaliser les énoncés et de les prouver.

L'objectif de ce travail est l'étude et la conception de méthodes permettant, avec l'aide d'un assistant de preuves, de prouver complètement des algorithmes probabilistes.

On procédera aux étapes suivantes :

- (Brève) étude bibliographique du sujet, notamment des exemples déjà prouvés.
- Prise en main de la bibliothèque **Alea** dédiée à la preuve en **Coq** de programmes probabilistes.
- Illustrer les méthodes de preuves par quelques exemples simples.

3 Pré-requis pour ce travail

Il n'existe pas de pré-requis pour ce sujet. L'étudiant doit être motivé pour apprendre à formaliser les algorithmes, à apprendre quelques éléments de probabilité et pour se former à la programmation/formalisation en utilisant l'assistant de peuves Coq. Il sera integré dans le groupe de travail AlgoProof et travaillera en étroite collaboration avec les membres du groupe.

4 Références bibliographiques

- Interactive Theorem Proving and Program Development. Coq'Art : The Calculus of Inductive Constructions, Y. Bertot and P.Castéran, Springer Verlag.
  (version en français disponible sur `www.labri.fr/∼casteran/CoqArt/coqartF.pdf`.)
- Proofs of randomized algorithms in Coq, P. Audebaud and C. Paulin, `hal.inria.fr/inria-00431771/en`
- Page web de l'assistant de preuves Coq : `coq.inria.fr/`.
- Page web de la bibliothèque Alea : `www.lri.fr/∼paulin/ALEA/`