Nom et Numéro de l'école doctorale: école doctorale de mathématiques et informatique de Bordeaux, ED-39)

Nom de l'unité de recherche: Laboratoire Bordelais de Recherche en Informatique (LaBRI)

Equipe : Méthodes Formelles

Localisation: Bordeaux - France

Nom du directeur de thèse et du co-directeur s'il y a lieu: Mohamed Mosbah et Pierre Castéran

Adresse courriel du contact scientifique : mosbah@labri.fr, casteran@labri.fr

Titre de la thèse : Environnement de preuves d'algorithmes distribués

Description synthétique du sujet

Prouver la correction d'un algorithme est l'une des tâches les plus importantes et les plus difficiles en informatique. Si des solutions et des outils standards acceptables existent pour l'algorithmique séquentielle classique, prouver la correction d'un algorithme distribué reste une tâche extrêmement difficile en raison de la complexité des intrinsèque des environnements distribués (synchronisme, non déterminisme, absence d'horloge globale). Ceci continue de stimuler une intense activité de recherche autour cette thématiques.
Nous proposons dans le cadre de cette thèse une méthode originale permettant d'aborder ce problème à un niveau d'abstraction élevé, ce qui permet de maitriser la complexité des systèmes distribués. Plus précisément, nous proposons d'intégrer les preuves en utilisant le modèle des calculs locaux. Le travail consiste donc, à définir une méthodologie générale de preuves d'algorithmes distribués décrits par des calculs locaux.

Description détaillée du sujet:

Les systèmes de réécriture de graphes, et plus généralement les calculs locaux, constituent un modèle formel solide pour exprimer à un bon niveau d'abstraction les algorithmes distribués. Dans ce modèle, un système distribué est représenté par un graphe étiqueté, connexe, et non orienté, où les sommets correspondent aux processeurs et les arêtes aux canaux de communication. L'étiquette d'un sommet (resp. d'une arête) code l'état du processeur (resp. du lien de communication) correspondant. Un calcul sur un système distribué (ou un algorithme distribué), qui consiste donc à faire évoluer ces états, peut être décrit par des règles de réécriture d'étiquettes de graphes. Chaque règle, définie par un graphe connexe et deux étiquetages de ce graphe, traduit un pas élémentaire du calcul effectué sur une portion locale du graphe. Cette représentation de haut niveau a permis d'étudier, d'analyser et d'obtenir des résultats nouveaux pour plusieurs problèmes de l'algorithmique distribuée comme l'élection, le nommage, le calcul d'un arbre recouvrant, la détection de la terminaison ou bien la reconnaissance de certaine propriétés du réseau.

De plus cette approche permet d'offrir un codage unifié et relativement intuitif pour prouver les algorithmes distribués en se ramenant à des preuves de terminaison de systèmes de réécriture et des preuves de validité d'invariants (qui se font actuellement manuellement). L'objectif de cette thèse est justement d'étudier et de développer, dans ce contexte, un environnement de preuves pour les algorithmes distribués. Il s'agit de définir une méthodologie générale de preuve et de s'appuyer sur des outils d'aide à la preuve existants (e.g. Coq) pour automatiser la vérification et la validation de ces preuves. La manipulation des règles de réécritures peut se faire à l'aide d'un langage, appelé

Lidia, que nous avons développé et qui offre une interface syntaxique pour décrire les algorithmes distribués. Lidia est fondé sur une extension de la logique du premier ordre qui peut exprimer les pré-conditions, actions des règles d'un système de réécriture.

Ce langage va évoluer vers un langage de programmation des calculs locaux. Prouver qu'un algorithme distribué exprimé en Lidia est conforme à une spécification peut être un travail long, contenant de nombreux calculs, et pouvant être entaché d'erreurs ou d'omissions s'il est fait " sur le papier " (à la main). L'ambition du travail proposé est de construire un outil de travail facilitant la preuve de correction de tel ou tel algorithme, mais également des propriétés génériques de telle ou telle classe de systèmes de réécriture.

Pour construire cet outil, nous utiliserons l'assistant de preuves Coq (http://coq.inria.fr) avec lequel de nombreux travaux sur la validation de programmes ont déjà été menés. Le travail consistera à exprimer en Coq une sémantique de Lidia, puis à prouver les propriétés des programmes permettant de construire et valider des outils d'aide à la preuve d'algorithmes distribués.
Plusieurs communautés d'informatique s'intéressent à cette thématique. Les techniques à utiliser seront similaires à celles du projet Proval de l'INRIA Futurs:
http://www.inria.fr/futurs/recherche/les-equipes-de-recherche/PROVAL_page

La bibliographie se trouve sur le site :
[1] http://www.labri.fr/visidia

Liste des projets en relation avec le sujet (ANR, Projet européen, ...)
Ce travail s'inscrit dans le cadre des ANR RIMEL (LaBRI, LORIA, entreprise CLEARSY) et A3PAT (Cedric, INRIA Sophia-Antipolis, LaBRI, LRI-PCRI)

Connaissance et compétences requises:

Une culture en algorithmique distribuée est requise pour cette thèse, ainsi que des notions de base sur les techniques de preuve et les langages de programmation. Il est souhaitable que le candidat possède une formation en informatique fondamentale notamment en algorithmique, graphes et systèmes de réécriture.