Lot 4: Technologie et Modélisation

Partenaires impliqués : LSV, PCRI, LORIA, FT R&D, Paris 7

Averroes, T0+18, Juin 2004

Décomposition du Lot

- Sous-lot 4.1 : Modélisation Compositionnelle
- Sous-lot 4.2 : Probabilités
- Sous-lot 4.3 : Complexité en espace et en temps

Sous-Lot 4.1 : Modélisation Compositionnelle

Idée : Etant données une composition d'automates $A_1|A_2|\cdots|A_n$, et une propriété φ, éviter de construire l'espace des états du réseau global en "incorporant" chaque automate dans la formule :

$$(A_1|A_2|\cdots|A_n) \models \varphi \text{ ssi } (A_1|A_2|\cdots|A_{n-1}) \models \varphi/A_n.$$

A la fin, on a à verifier :

$$\text{nil} \models ((\ldots(\varphi/A_n)\ldots/A_2)/A_1).$$

Problème ramené à un probleme de satisfiabilité d'une contrainte.

Extension de HCMC aux p-automates

Probleme : Comment intégrer la méthode décompositionnelle aux p-automates (automates temporisés avec paramètres) ?

Approche :

- Coder les paramètres sous forme de chronomètres (i.e., horloges qui peuvent s'arrêter)
- implémentation d'une sur-approximation des opérations sur les ensembles de configurations (basées sur les DBM - Difference Bounded Matrix)

Sous-lot 4.1 : Etat d'avancement

- Fourniture :

  F4.1.1 “Vérification compositionnelle des p-automates”,
  B. Bérard et F. Laroussinie

- Workplan :
  Intégration d'une bibliothèque de polyhèdres en cours de déboggage (validation prévue fin 2004 ; cf. lot 5)

Sous-lot 4.2 : Probabilités

- Motivation : Spécification et modélisation de systèmes temps-réel nécessite souvent de faire intervenir des facteurs probabilistes dans la modélisation de l'environnement et des comportements (ex: pannes).
- Objectif :
  - Réfléchir aux principes d'extensions probabilistes des p-automates.
  - Mettre en place des extensions de bibliothèques Coq/Elan pour raisonner sur des objets probabilistes ;
  - Utilisation pour modélisation et la vérification d'un protocole probabiliste (ex: CSMA/CD).

Extensions probabilistes des p-automates

- Probleme 1 : Combinaison avec le non-determinisme (Markov Decision Process vs. Markov Chain)
- Probleme 2 : Integration des contraintes temporelles (Discrétisation du temps, Compilation du graphe des zones en chainage avant)
- Etudes de cas
  - Sur la specification de Nicollin-Sifakis-Yovine, étude réalisée avec les outils HYTECH et PRISM.
  - Sur la spécification de Duflot-Messika-Picaronny, étude réalisée avec les outils PRISM et APMC (LRI/Paris7)

Sous-lot 4.2: probabilités (suite)

- bibliothèques Coq pour les notions probabilistes élémentaires
  - utilise une représentation des programmes par des distributions (suivant une idée de Kozen).
  - lemmes permettant d'estimer la probabilité pour un programme de vérifier une propriété.
  - quelques exemples simples : marche aléatoire, distribution de Bernouilli.
- extension de ELAN pour le prototypage de syst. probabilistes

  Ajout au langage de stratégie d'opérateurs permettant des choix probabilistes (fourniture en cours de rédaction).

Sous-lot 4.2 : Fournitures

- P-automates probabilistes :
  - F4.2.1 “Vérification du protocole CSMA/CD sous PRISM”, M. Duflot, S. Messika, and C. Picaronny.
  - F4.2.2 “Probabilistic Model Checking of the CSMA/CD protocol using PRISM and APMC”, M. Duflot, L. Fribourg, T. Herault, R. Lassaigne et al.
  - F4.2.3 “Parametric and probabilistic verification of NSY’s model of the CSMA/CD protocol”, L. Fribourg, S. Messika, and C. Picaronny.
- Coq : bibliothèque disponible à l’adresse http://www.lri.fr/ paulin/ALEA/HTML/
- ELAN : En cours de rédaction, par Florent Garnier (LORIA)

Sous-lot 4.2 : Workplan

- P-automates probabilistes :
  - Manipulation des paramètres
  - Isolation des sources de non-determinisme.
- Coq
  - Affiner le modèle sur ex. plus conséquents (recherche de coupure minimale dans un graphe).
  - Faisabilité de l'approche pour des systèmes de transitions probabilistes (modélisation CSMA/CD)
  - Etude de la traduction des p-automates probabilistes CALIFE (avec x:=random).
- ELAN : Prototyper protocoles relatifs au projet (CSMA/CD).

Sous-lot 4.3: complexité en espace et temps

Extraction d'informations sémantiques visant la consommation de ressources en temps et en espace, à partir d'un programme spécifié par un langage fonctionnel du 1er ordre ou d'une preuve de correction de programme faite en Coq.

- Systeme d'analyse pour les prog. fonctionnels du 1er ordre
  Prototype/logiciel ICAR.
- application aux systèmes à codes mobiles
  En cours.

Sous-lot 4.3 : Etat d'avancement

- Fourniture
  F.4.3.1 "Un système d'analyse pour les programmes fonctionnels du 1er ordre", J.-Y. Marion.

- Workplan
  Etendre les méthodes d'analyse des ressources à l'analyse d'un bytecode