APPROCHES DÉDUCTIVES POUR LA VÉRIFICATION DE PROCESSUS

Sujet

Les algèbres de processus comme CCS de Milner permettent de modéliser et de vérifier des systèmes parallèles communicants. Elles sont définies comme des structures :

$$\langle \mathscr{P}, \Sigma, eqs \rangle$$

où :

— les termes $\mathscr{P} = \{P, Q, R, \ldots\}$ sont des processus ;

— Σ est l'ensemble des opérateurs entre termes :
$\Sigma = \{., +, ||, |||, \backslash A, /A, \ldots\}$ où $A = \{a, b, c, \ldots\}$ est un ensemble de noms d'actions ;

— *eqs* est l'ensemble des équations sur les opérateurs du langage, pour un jeu de relations d'équivalence donné.

Nous considérons ici les algèbres telles que CCS ou LOTOS. Nous excluons les algèbres mobiles comme le π-calcul. Milner a défini un ensemble de relations d'équivalence (équivalence forte $\sim$, équivalence observationnelle $\approx$, congruence observationnelle $=$). Ces relations sont définies sur la sémantique opérationnelle des processus donnée sur des systèmes de transitions étiquetées (LTS). En pratique, ces relations sont également vérifiées sur les LTS.

L'objectif de ce stage consiste à construire un outil de déduction automatique pour vérifier ces relations, sans chercher à traduire les processus en systèmes de transitions. Par exemple, pour la relation de congruence observationnelle $=$, on a les axiomes suivants (extrait) :

$$P + 0 = P \quad (1)$$
$$P + P = P \quad (2)$$
$$P + Q = Q + P \quad (3)$$
$$P + (Q + R) = (P + Q) + R \quad (4)$$
$$a.\tau.P = a.P \quad (5)$$
$$P + \tau.P = \tau.P \quad (6)$$
$$P||0 = 0 \quad (7)$$
$$P|||0 = P \quad (8)$$
$$a.(P + \tau.Q) + a.Q = a.(P + \tau.Q) \quad (9)$$

En général, on a $a.(P + Q) \neq a.P + a.Q$ (10), mais aussi $a.(b.P + b.Q) \neq a.b.P + a.b.Q$ (11).

La congruence observationnelle de Milner est calculable de façon efficace sur les LTS, mais cette approche se limite de façon évidente aux cas des processus explicites pour lesquels on sait générer un LTS fini et en temps raisonnable. D'autre part, si la relation (10) est souhaitée, la relation (11) ci-dessus montre que la congruence observationnelle n'est en réalité pas observationnelle. Rien ne permet de distinguer ces deux processus. D'autres équivalences ont été proposées, comme les équivalences de test. En revanche, la vérification de ces équivalences de test est beaucoup moins efficace. L'objectif sera, à partir d'axiomatisations existantes, d'étudier leur mise en œuvre dans l'outil Coq. Dans un premier temps, on fera les preuves manuellement, puis dans un second temps, on construira une procédure de preuve automatique.

Remarques additionnelles

Le stage s'effectuera au sein de l'équipe MaREL du LIRMM (à Montpellier) et en collaboration avec le LGI2P de l'IMT Mines Alès. L'encadrement sera réalisé par :

— David Delahaye (Université de Montpellier, LIRMM, David.Delahaye@lirmm.fr) ;

— Thomas Lambolais (IMT Mines Alès, LGI2P, Thomas.Lambolais@mines-ales.fr).