Sujet de stage L3 ENS
année 2013 - 2014

Didier Galmiche - Dominique Larchey-Wendling
Equipe TYPES, LORIA UMR 7503

Titre : Axiomes pour la logique de séparation

Thématique.

Un défi majeur pour appréhender les problèmes posés par la complexité des systèmes actuels est de proposer de nouveaux cadres formels et de nouvelles méthodes d'analyse et de conception qui intègrent dès l'origine, de manière globale et intrinsèque, les liens et interactions qui existent entre les aspects statiques et dynamiques d'un système. Nous souhaitons proposer des cadres formels et des méthodes capables de travailler à la fois selon trois dimensions transversales : une première liée à des propriétés de nature spatiale (distribution, mobilité dans l'espace), une deuxième liée à des propriétés de nature temporelle (par exemple, l'évolution du système vers un état stable), et enfin, une troisième pour rendre compte de problèmes en termes quantitatifs et pas uniquement qualitatifs (par exemple, toutes les trois opérations de lecture, le système vérifie la présence d'une opération d'écriture en attente).
La notion de ressource et les problématiques liées à leur gestion sont au coeur de notre approche. Nous entendons ici par ressources aussi bien des entités physiques (un circuit électronique, un processeur) que des entités abstraites (une structure de données, un processus). On s'intéresse plus particulièrement à des phénomènes de production / consommation (jetons dans un réseau de Petri), de partage / séparation (zones de mémoire, contrôles d'accès), de distribution spatiale et de mobilité (processus mobiles, systèmes embarqués). Presque tout objet présentant des propriétés de ressources, les logiques et modèles de ressources suscitent depuis quelques années un vif intérêt dans le domaine de l'analyse et de la conception de systèmes complexes.
Dans le contexte des logiques de ressources, on s'intéressera plus particulièrement aux *logiques de séparation* et en particulier la logique BI [13] (Logic of Bunched Implications) et ses variantes, qui incluent un opérateur de composition s'interprétant en termes de partage et de séparation de ressources. D'autres logiques sous-structurelles, dont la logique linéaire [8], entrent aussi dans cette catégorie : leur formalisme permet d'exprimer des propriétés de ressources, comme par exemple le partage, la séparation, la localisation, le comptage, etc.

Sujet.

La logique BI se décline en une version intuitionniste [14] et une version classique [6] qui se distinguent par les propriétés de leurs opérateurs additifs. Dans sa version classique appelée Boolean BI (BBI) elle constitue le noyau autour duquel sont contruites les logiques de séparation [9].
Plusieurs méthodes de preuves existent pour BI et Boolean BI. Par exemple, le calcul des séquents avec "bunches" [14] pour BI, la méthode des tableaux avec contraintes sémantiques pour BI [7] et BBI [10], ou encore des méthodes à base de Display Logic [1] pour BI/BBI. Bien que la version intuitionniste de BI soit décidable [7], et bien que la validité soit décidable dans certaines logiques spatiales [4], plusieurs résultats d'indécidabilité ont récemment été établis dans le cas de la logique BBI [2, 11, 12].

Lors de notre étude de la recherche de preuves dans Boolean BI [10], nous avons découvert un plongement surprenant de BI (intuitionniste) dans BBI. Nous avons également mis en évidence l'existence

potentielle de ressources inversibles dans les modèles engendrés par la recherche de preuves. Ces modèles sont construits à partir de contraintes sémantiques déduites de la décomposition des formules logiques de BBI. Ainsi il semble important de prendre en compte l'inversibilité de certaines ressources et proposer des modèles concrets qui traitent de ressources inversibles non-triviales.
Nous avons développé une preuve formelle en Coq de la correction et de la complétude de BBI basée sur la méthode des tableaux sémantiques avec labels et contraintes. Cette preuve prend en compte les ressources inversibles.[1] D'autres travaux [5] explorent plusieurs pistes d'axiomatisation des algèbres de séparation. Les auteurs identifient les axiomes de *non-inversibilité*, *positivité*, d'*incompatibilité*, de *croisement* et *découpage infini*. Ces travaux sont également accompagnés de développement formels en Coq.

L'objectif de ce stage est d'explorer plus avant ces axiomes dans le cadre de BBI et des algèbres de séparation. Il pourra conduire à proposer des modifications à la méthode des tableaux existantes pour y intégrer ces axiomes, en préservant si possible la complétude. L'étude des liens logiques entre ces axiomes ou des combinaisons de ces axiomes pourra aussi être abordée.

Renseignements. Le stage aura lieu au sein de l'équipe TYPES du LORIA à Nancy. Pour tout renseignement complémentaire sur ce sujet, contacter D. Galmiche et D. Larchey-Wendling (e-mail : galmiche@loria.fr, larchey@loria.fr).

Références

[1] James Brotherston. Bunched logics displayed. *Studia Logica : Special Issue on Recent Developments related to Residuated Lattices and Substructural Logics*, 2011. Awaiting publication.

[2] James Brotherston and Max I. Kanovich. Undecidability of propositional separation logic and its neighbours. In *25th IEEE Symposium on Logic in Computer Science, LICS 2010*, pages 130–139. IEEE Computer Society, 2010.

[3] Luís Caires and Étienne Lozes. Elimination of quantifiers and undecidability in spatial logics for concurrency. *Theor. Comput. Sci.*, 358(2-3) :293–314, 2006.

[4] Cristiano Calcagno, Hongseok Yang, and Peter W. O'Hearn. Computability and complexity results for a spatial assertion language for data structures. In *APLAS*, pages 289–300, 2001.

[5] Robert Dockins, Aquinas Hobor and Andrew W. Appel. A Fresh Look at Separation Algebras and Share Accounting. In *APLAS*, pages 161–177, 2009.

[6] Didier Galmiche and Dominique Larchey-Wendling. Expressivity properties of Boolean BI through relational models. In *FSTTCS*, volume 4337 of *LNCS*, pages 357–368. Springer, 2006.

[7] Didier Galmiche, Daniel Méry, and David Pym. The semantics of BI and resource tableaux. *Math. Struct. in Comp. Science*, 15(6) :1033–1088, 2005.

[8] Jean-Yves Girard. Linear logic. *TCS*, 50(1) :1–102, 1987.

[9] Samin S. Ishtiaq and Peter W. O'Hearn. Bi as an assertion language for mutable data structures. In *28th ACM Symposium on Principles of Programming Languages, POPL 2001*, pages 14–26, 2001.

[10] Dominique Larchey-Wendling and Didier Galmiche. Exploring the relation between Intui. BI and Boolean BI : an unexpected embedding. *Math. Struct. in Comp. Science*, 19(3) :435–500, 2009.

[11] Dominique Larchey-Wendling. An alternative direct simulation of Minsky machines into classical bunched logics via group semantics. *Electr. Notes Theor. Comput. Sci.*, 265 :369–387, 2010.

[12] Dominique Larchey-Wendling and Didier Galmiche. The Undecidability of Boolean BI through Phase Semantics. In *25th IEEE Symposium on Logic in Computer Science, LICS 2010*, pages 147–156. IEEE Computer Society, 2010.

[13] Peter O'Hearn and David Pym. The logic of Bunched Implications. *Bulletin of Symbolic Logic*, 5(2) :215–244, 1999.

[14] D. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*. Kluwer Academic Publishers, 2002.

[1] `http ://www.loria.fr/~larchey/BBI.`