Resource Tree and Logics for Distribution
- abstract -

N. Biri and D. Galmiche

LORIA - Université Henri Poincaré
54506 Vandœuvre-lès-Nancy Cedex, France
biri{galmiche}@loria.fr

1 Abstract

The notion of *resource* is a basic one in many fields, including computer science. The location, ownership, distribution, access to and, indeed, consumption of, resources are central concerns in the design of systems (such as networks) and also of programs which access memory and manipulate data structures (such as pointers). The logic of Bunched Implications (BI), that is a resource-aware logic in which additive ($\wedge$,$\rightarrow$) and multiplicative connectives ($*$, $-\!\!*$) cohabit [9], appears as a kernel logic of resource (de)composition as illustrated by separation logics [7,8,10] and also by spatial logics for distributed and mobile computations [4]. It is natural, in this setting, to consider primitive notions of location or distribution and then to define a new separation logic, based on BI logic extended with a location modality, for reasoning on distributed resources. In addition, we aim to define a resource tree model for this logic that allows to reason and prove properties on based-on resource trees structures.
In this context, it is important to define models that well reflect structures but also logics that are enough expressive to represent data properties and enough restricted to decide if a given model satisfies a formula or if some properties entail other properties. We observe in recent works on tree models (and their related logics) some limits for information representation such as the difficulty to represent complex data inside nodes [3] and the choice of a resource composition that is not partial, knowing that partiality enables to ensure that substructures are disjoints. Therefore, we study a new data model, called resource tree, that is a labelled tree structure in which nodes contain resources that are elements of a partially defined monoid and we show how and why it is an appropriate proposal to deal with resource distribution. Then, we define a tree structure that represents complex information, through resources inside nodes, and also distinguishes the structure and the information it contains. Moreover, we can alter an existing structure and characterize inconsistent trees (not valid according to a specification).
In order to define a logic for resource trees we consider the extension of the BI logic with a modality for locations (BI-Loc). It can be viewed as a separation and spatial logic: the BI's multiplicatives naturally introduce the notion of resource separation and the location modality allows to gather resources in some locations and thus to introduce a notion of spatial distribution of resources. The use of a partial composition on resources and the introduction of a location modality in a resource-aware logic [5] are key points in this work.
We first define what a resource tree is and illustrate its specific features. Then, we present the related separation logic BI-Loc and in order to analyze the decidability for resource trees against this logic, we show that BI is decidable by model-checking for partial resource monoids that satisfy some specific conditions. This result is extended to resource trees and its separation logic. Details are given in [2]. In addition, this model is extended with quantifications on locations and paths and we propose new results about (un)decidability of satisfaction and validity in BI-Loc with such extensions. Moreover, we relate the logics and the models to the specification and verification

of properties of semi-structured data and analyze the relationships with other models and logics dealing with the notions of location [3] and hierarchy of resources [1]. Finally we study a theorem proving approach, starting from some recent results about decidability of BI and a new based-on partially defined monoids semantics of BI that is complete [6].

References

1. A. Ahmed, L. Jia, and D. Walker. Reasoning about hierarchical storage. In *18th Symposium on Logic in Computer Science*, Ottawa, Canada, 2003.
2. N. Biri and D. Galmiche. A Separation Logic for Resource Distribution. In *23rd Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS'03, LNCS 2914*, pages 23–37, December 2003. Mumbai, India.
3. C. Calcagno, L. Cardelli, and A. Gordon. Deciding validity in a spatial logic for trees. In *ACM Sigplan Workshop on Types in Language Design and Implementation, TLDI'03*, New Orleans, USA, 2003.
4. L. Cardelli and A.D. Gordon. Anytime, anywhere - modal logics for mobile ambients. In *27th ACM Symposium on Principles of Programming Languages, POPL 2000*, pages 1–13, Boston, USA, 2000.
5. D. Galmiche and D. Méry. Connection-based proof search in propositional BI logic. In *18th Int. Conference on Automated Deduction, CADE-18, LNAI 2392*, pages 111–128, 2002. Copenhagen, Danemark.
6. D. Galmiche, D. Méry, and D. Pym. Resource Tableaux (extended abstract). In *16th Int. Workshop on Computer Science Logic, CSL 2002, LNCS 2471*, pages 183–199, September 2002. Edinburgh, Scotland.
7. S. Ishtiaq and P. 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, London, UK, 2001.
8. P. O'Hearn, J. Reynolds, and H. Yang. Local reasoning about programs that alter data structures. In *15th Int. Workshop on Computer Science Logic, CSL 2001, LNCS 2142*, pages 1–19, Paris, France, 2001.
9. D.J. Pym. *The Semantics and Proof Theory of the Logic of Bunched Implications*, volume 26 of *Applied Logic Series*. Kluwer Academic Publishers, 2002.
10. J. Reynolds. Separation logic: A logic for shared mutable data structures. In *IEEE Symposium on Logic in Computer Science*, pages 55–74, Copenhagen, Danemark, July 2002.