Verification of Distributed Algorithms by Construction

Dominique Méry
Université de Lorraine, LORIA UMR7503

October 24, 2018

Abstract

The verification of distributed algorithms is a challenge for formal techniques supported by tools, as model checkers and proof assistants. The difficulties, even for powerful tools, lie in the derivation of proofs of required properties, such as safety and eventuality, for distributed algorithms. Verification by construction can be achieved by using a formal framework in which models are constructed at different levels of abstraction; each level of abstraction is refined by the one below, and this refinement relationships is documented by an abstraction relation namely a gluing invariant. The highest levels of abstraction are used to express the required behavior in terms of the problem domain and the lowest level of abstraction corresponds to an implementation from which an efficient implementation can be derived automatically. In this talk, we will show a methodology based on the general concept of refinement and used for developing distributed algorithms satisfying a given list of safety and liveness properties. The modelling methodology is defined in the Event-B modelling language using the IDE RODIN. More precisely, we show how Event-B models can be developed for specific problems and how they can be simply reused by controlling the composition of state-based models through the refinement relationship. Consequently, we obtain a redevelopment of *correct-by-construction* existing distributed algorithms and a framework for deriving new distributed algorithms (by integrating models) and for ensuring the correctness of resulting distributed algorithms by construction. We illustrate our methodology using the classical problem of communication in a network. These works have been carried out in collaboration with J.-R. Abrial, M. Andriamiarina, D. Cansell, P. Castran, Y. Mtivier, M. Mosbah, M. Poppleton, M. Tounsi, N. Singh and partners of the ANR project RIMEL (http://rimel.loria.fr). Resources are available at the link http://eb2all.loria.fr and are part of the current project on developing an atlas of correct-by-construction distributed algorithms.