SMT-based approaches to Model Checking of Distributed Broadcast Algorithms – Work In Progress –

Francesco Alberti[1], Silvio Ghilardi[2]*, Andrea Orsini[2] and Elena Pagani[2]

[1] Fondazione Centro San Raffaele, Milano, Italy
alberti.francesco@hsr.it
[2] Università degli Studi di Milano, Milano, Italy
silvio.ghilardi@unimi.it, andrea.orsini2011@gmail.com, pagani@di.unimi.it

Abstract

The validation of distributed algorithms is a crucial, although challenging, task. The processes executing these algorithms communicate to one another, their actions depend on the messages received, and their number is arbitrary. These characteristics are captured by so called reactive parameterized systems. The task of validating or refuting properties of these systems is daunting, due to the difficulty of limiting the possible evolutions, thus having to deal with genuinely infinite-state systems.

In this paper, we consider distributed algorithms to solve the reliable broadcast problem in the presence of crash, send-omission, and byzantine failures. We study the properties of these algorithms using Model Checker Modulo Theories (MCMT). MCMT is able to verify safety properties of infinite-state reactive parameterized systems, for any number of processes. It adopts a pure SMT (Satisfiability Modulo Theories) approach, due to its flexibility. It uses some form of abstractions, and involves acceleration mechanisms in order to increase computation efficiency.

In this work, we study how to model the algorithms in MCMT according to two paradigms: array-based systems and counter abstraction. The former uses unbounded arrays to represent the states of the processes. The latter exploits a characteristic of the considered algorithms, which consists in determining the behavior of the processes depending on the number of messages they receive from other processes (threshold-guarded algorithms). The algorithms are modeled according to both paradigms, or using a hybrid approach mixing arrays with counter abstraction. We discuss the rationale of our modeling choices and show how to use the characteristics of MCMT to perform the validation. We report a performance evaluation of the computation with the different models, and (in the counter abstraction paradigm) compare the results with equivalent modelization in both Z3 and nuXmv, obtained by translating our models.

Keywords: reactive parameterized systems; SMT-based model checking; fault-tolerant broadcast algorithms; array-based systems; counter abstraction.

*Reference author