Model Checking of Fault-tolerant Distributed Algorithms

Josef Widder
Embedded Computing Systems group at TU Wien

Where: Jakob-Haringer-Str. 2, Raum T03

When: Tuesday, June, 2015, 09:15 – 12:00

This guest lecture is part of the Model Checking Course (taught by Ana Sokolova), but it provides a self-contained tutorial on the topic and we welcome all members of the department to attend

Fault-tolerant distributed algorithms provide a system designer with a mechanism for constructing reliable computing systems. In this talk, we will introduce basic notions such as timing assumptions, fault assumptions, and classic problems in this area. By reviewing classic paper & pencil correctness arguments, we motivate the use of automated verification methods such as model checking.

The first step towards automated verification is adequate modeling. Thus, we explain how to encode the semantics of fault-tolerant distributed algorithms in Promela, the input language of the Spin model checker.

Then, we introduce an automated parameterized verification method for fault-tolerant distributed algorithms (FTDA): FTDAs are parameterized by both the number of processes and the assumed maximum number of faults. At the center of our technique is a parametric interval abstraction (PIA) where the interval boundaries are arithmetic expressions over parameters. Using PIA for both data abstraction and a new form of counter abstraction, we reduce the parameterized problem to finite-state model checking. We demonstrate the practical feasibility of our method by verifying safety and liveness of several fault-tolerant broadcasting algorithms, and finding counter examples in the case where there are more faults than the FTDA was designed for.

Josef Widder is assistant professor (Privatdozent) in the Embedded Computing Systems group at TU Wien. In the past, he worked at Ecole polytechnique, Texas A&M University, and the Formal Methods in Systems Engineering group at TU Wien. His primary area of interest is the theoretical approach to distributed algorithms, currently focussing on automated verification of fault-tolerant distributed algorithms.

UNIVERSITÄT SALZBURG

Software Systems Center
Colloqium Series

host: Ana Sokolova