TITLE: "Relational Invariants for Verification of Parameterized Timed Systems"

ABSTRACT: Program verification can be viewed as finding the solutions for a set of relational symbols in a possibly recursive set of constraints (Horn clauses). There are various techniques and tools available that are able to solve a given set of recursive Horn clauses. In a concurrent setting where there are multiple processes running in parallel, the classical approaches of Owicki-Gries and Assume-Guarantee have been exploited to express the concurrent program using Horn clauses. In this work we address the problem of verifying parameterized timed and untimed systems.

Verification of such systems raise new challenges as it requires modeling of time and an infinite number of processes. I will present how we model timed automata in the formal verification framework Eldarica by Horn clauses. I will then elaborate on the concept of relational invariants which allows us to take the relations among different replicated processes into account. Relational invariants enabled our tool Eldarica to successfully solve a set of parameterized (un-)timed benchmarks.

Joint work: Philipp Ruemmer, Pavle Subotic, Viktor Kuncak, Wang Yi