From Symbolic Reachability to Inductive Invariants: Narrowing-Based Verification of Concurrent Systems

Datum	15.10.2026
Subjekt	IMDEA Software Institute
Region	Španielsko
Kategorie	IT a komunikácie, Technológie, Veda a výskum

The verification of concurrent systems with potentially infinite state spaces remains a recurring challenge in formal verification.

One way to address this problem is through symbolic techniques that explore representations of sets of states rather than individual executions. In this seminar, we present a narrowing-based approach to the symbolic verification of concurrent systems specified as rewrite theories in Maude. We first introduce the main ideas behind symbolic reachability analysis, constrained narrowing, and folding techniques, showing how they can be used to explore infinite-state systems. The main focus of the seminar is DM-Check, a deductive model checker that combines narrowing-based symbolic exploration with the inductive theorem proving capabilities of NuITP. Through two representative case studies, we illustrate how DM-Check supports the semi-automated verification and generation of inductive invariants, enabling users to establish safety properties that would be difficult to verify through direct state-space exploration alone. Finally, we discuss current challenges and possible directions for future research.

https://software.imdea.org/events/invited-talks/2026/11-19