ICT25-051 - Verifying Without Loss of Generality

Zusammenfassung

Da Hardware häufig in sicherheitskritischen Bereichen eingesetzt wird, ist ihre Zuverlässigkeit von größter Bedeutung: Die Kosten für Fehlfunktionen oder Sicherheitsverletzungen können immens sein, was für den Einsatz von mathematisch rigorosen und automatisierten Methoden zur Gewährleistung der Korrektheit von Hardware-Designs spricht. Allerdings sind bestehende automatisierte Verifikationstechniken oft nicht skalierbar, weshalb meist nur eine eingeschränkte Anzahl an Heuristiken und Reduktionen eingesetzt wird.

Um diese Einschränkungen zu überwinden, schlagen wir einen Ansatz vor, der es ermöglicht, Korrektheitsbeweise "ohne Einschränkung der Allgemeinheit" (WLOG) durchzuführen. Das bedeutet, dass die Analyse auf einen speziellen Fall eingegrenzt wird, doch die Korrektheitsgarantien auch für alle anderen Fälle halten. Wir werden unseren Ansatz in bestehende Verifikationstools integrieren (was die Verifikation zuvor nicht verifizierbarer Designs ermöglichen soll) und Werkzeuge bereitstellen, um zu garantieren, dass die Reduktionen und Einschränkungen mathematisch korrekt sind. Dies wird letztendlich in einer erhöhten Zuverlässigkeit digitaler Schaltungen resultieren.

Wissenschaftliche Disziplinen:
Formal languages (40%) | Theoretical computer science (50%) | Computer aided design (CAD)

Keywords:
Formal verificationModel CheckingReductionCertification

Principal Investigator: Adrian Rebola Pardo

Institution: TU Wien

Co-Principal Investigator(s): Georg Weissenbacher (TU Wien)

Status: Laufend (01.01.2026 - 31.12.2029)
GrantID: 10.47379/ICT25051

Weiterführende Links zu den beteiligten Personen und zum Projekt finden Sie unter
https://www.wwtf.at/funding/programmes/ict/ICT25-051/