Karlsruher Institut für Technologie

Institut für Theoretische Informatik (ITI)
Anwendungsorientierte Formale Verifikation
Prof. Dr. Bernhard Beckert

Masterarbeit – Praxis der Forschung

Hyper Test Tables

Background. Hyper properties became very popular in the last years, because of their expressive power. The core of hyper properties is the possibility to (universal and existential) quantified over program traces. For example, this enables the specification of refinement (“forall runs in the old software revision, exists a run in the new revision“) or:

> Hyperproperties can express security policies, such as secure information flow and service level agreements, that trace properties cannot.
>
> — Clarkson and Schneider in *Hyperproperties. JCS 18. 2010.*

Goal. The goal is a table-based specification language, that (a) supports hyper properties and (b) is decidable by state-of-the-art tools (model checker or SMT solver).

Task. Your task is to understand the current work of generalized test tables, HyperLTL and HyperCTL. You define the syntax and sematic of the specification language and implement a decision procedure for proving the conformance of reactive system to your specification.

#			INPUT				OUTPUT		◷	
	Level	WPReady	Position	Carry	_state	Turn	Lower	Vacuum		
0	::	::	::	::	—	::	::	::	DWAIT	
1	Up	MetalReady	TRUE		Crane_Go_Up				1	ω
2	—	—	—	—		Right			≥ 0	
3			Magazine						1	
4				FALSE		Stop	TRUE	On	≥ 0	
5				TRUE			TRUE		1	
6	Down			—			FALSE		≥ 0	
7	Up								1	
8	—					Left			≥ 0	
9			Conveyor						1	
10						Stop	TRUE		≥ 0	
11									1	
12								Off	1	
13	Down						FALSE		≥ 0	
14	Up								1	
15	—					Left			≥ 0	
16			Stamp						1	
17						Stop			1	
18	::	::	::	::	::	::	::	::	1	
19	::	::	::	::	—	::	::	::	DWAIT	

Your profile. Programming skills on Java required. Furthermore, you should be interested in formal logic, especially in automata theory and temporal logics. You should have completed the Formal Methods (Formale Systeme) Course at KIT or equivalent. Formal System 2 (Theory and Practise) are heavy benifical.

References. **(1)** Algorithms for Model Checking HyperLTL and HyperCTL*. Bernd Finkbeiner and César Sánchez. CAV 2015. **(2)** Temporal Logics for Hyperproperties. Michael Clarkson, et. al. POST 2014. **(3)** Model Checking Information Flow in Reactive Systems. Rayna Dimitrova et.al. VMCAI 2012. **(4)** Hyperproperties. Michael R. Clarkson and Fred B. Schneider. Journal of Computer Security 18 (2010) 1157–1210.

Kontakt

Alexander Weigl weigl@kit.edu Office: 50.34, R225