EAHyper:

Satisfiability, Implication, and Equivalence Checking of Hyperproperties

Bernd Finkbeiner, Christopher Hahn, and Marvin Stenger
Reactive Systems Group, Saarland University, Germany

The 29th International Conference on Computer Aided Verification
Heidelberg, Germany, 2017

Hyperproperties

Definition

A Hyperproperty $H \subseteq 2^{TR}$ is a set of sets of execution traces. [Clarkson, Schneider, '10]

Example

Observational Determinism: "Program appears deterministic to low security users."

Generalized Noninterference: ". . . additionally low-security outputs may not be altered by injection of high-security inputs."

A Logical Approach to Information-Flow Control

HyperLTL [Clarkson, Finkbeiner, Koleini, Micinski, Rabe, Sánchez, ’14]

MCHyper [Finkbeiner, Rabe, Sánchez, ’15]

HyperLTL

- LTL + explicit trace quatification:
  $\exists \pi. \exists \pi'. \ \square a_\pi \land \square \neg a_{\pi'}$
  satisfiable by $\{\{a\}^\omega, \{b\}^\omega\}$
- Observational Determinism:
  - $\forall \pi. \forall \pi'. \ \square (I_\pi = I_{\pi'}) \rightarrow \square (O_\pi = O_{\pi'})$
  - $\forall \pi. \forall \pi'. \ (O_\pi = O_{\pi'}) \ W \ (I_\pi \neq I_{\pi'})$

A Logical Approach to Information-Flow Control

HyperLTL [Clarkson, Finkbeiner, Koleini, Micinski, Rabe, Sánchez, ’14]
MCHyper [Finkbeiner, Rabe, Sánchez, ’15]

HyperLTL

- LTL + explicit trace quatification:
  $\exists \pi . \exists \pi' . \ \Box a_{\pi} \wedge \Box \neg a_{\pi'}$
  satisfiable by $\{\{a\}^{\omega}, \{b\}^{\omega}\}$
- Observational Determinism:
  - $\forall \pi . \forall \pi' . \ \Box (I_{\pi} = I_{\pi'}) \rightarrow \Box (O_{\pi} = O_{\pi'})$
  - $\forall \pi . \forall \pi' . \ (O_{\pi} = O_{\pi'}) \ W \ (I_{\pi} \neq I_{\pi'})$
- EAHyper: Which variation is stronger?

EAHyper: https://www.react.uni-saarland.de/tools/online/EAHyper

A satisfiability solver for the decidable fragment of Hyperproperties [Finkbeiner, H., ’16].

EAHyper: https://www.react.uni-saarland.de/tools/online/EAHyper

A satisfiability solver for the decidable fragment of Hyperproperties [Finkbeiner, H., ’16].

- Satisfiability Checking:
  - Have we made a mistake in the formalization?
  - Is our Hyperproperty unsatisfiable or trivially true?
  - Are our correctness requirements consistent with certain information-flow policies?

EAHyper: https://www.react.uni-saarland.de/tools/online/EAHyper

A satisfiability solver for the decidable fragment of Hyperproperties [Finkbeiner, H., '16].

- Satisfiability Checking:
  - Have we made a mistake in the formalization?
  - Is our Hyperproperty unsatisfiable or trivially true?
  - Are our correctness requirements consistent with certain information-flow policies?
- Implication and Equivalence Checking:
  - Can we avoid overhead in the verification process?
  - Which variation of a certain information-flow policy is stronger?

Benchmarks

Table: Random formulas benchmark: instances solved in 120 seconds and average wall clock time in seconds for 250 random formulas.

size	40	60	40	60	40	60	40	60	40	60	40	60	40	60	40	60	40	60
	∃0∀0		∃1∀0		∃2∀0		∃3∀0		∃4∀0		∃5∀0		∃6∀0		∃7∀0		∃8∀0	
solved			250	250	250	250	250	250	250	250	250	250	250	250	250	250	250	250
avgt			0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
	∃0∀1		∃1∀1		∃2∀1		∃3∀1		∃4∀1		∃5∀1		∃6∀1		∃7∀1		∃8∀1	
solved	250	250	250	250	250	250	250	249	250	250	249	247	250	248	249	247	247	248
avgt	0.01	0.01	0.01	0.01	0.02	0.02	0.02	0.05	0.02	0.06	0.02	0.01	0.02	0.01	0.13	0.02	0.04	0.08
	∃0∀2		∃1∀2		∃2∀2		∃3∀2		∃4∀2		∃5∀2		∃6∀2		∃7∀2		∃8∀2	
solved	250	250	250	250	248	249	249	247	247	247	248	246	246	246	244	246	244	247
avgt	0.01	0.01	0.01	0.01	0.03	0.12	0.03	0.01	0.26	0.02	0.32	0.02	0.09	0.02	0.02	0.02	0.05	0.03
	∃0∀3		∃1∀3		∃2∀3		∃3∀3		∃4∀3		∃5∀3		∃6∀3		∃7∀3		∃8∀3	
solved	250	250	250	250	249	247	248	246	247	245	245	246	245	246	244	247	243	246
avgt	0.01	0.01	0.01	0.01	0.03	0.02	0.07	0.02	0.06	0.03	0.14	0.05	0.17	0.08	0.23	0.16	0.45	0.25
	∃0∀4		∃1∀4		∃2∀4		∃3∀4		∃4∀4		∃5∀4		∃6∀4		∃7∀4		∃8∀4	
solved	250	250	250	250	250	246	247	246	245	246	244	247	245	247	244	245	0	0
avgt	0.01	0.1	0.01	0.01	0.02	0.01	0.21	0.03	0.35	0.09	0.23	0.28	0.46	1.01	0.98	2.41	–	–
	∃0∀5		∃1∀5		∃2∀5		∃3∀5		∃4∀5		∃5∀5		∃6∀5		∃7∀5		∃8∀5	
solved	250	250	250	250	249	247	248	247	243	245	245	246	0	0	0	0	0	0
avgt	0.01	0.01	0.01	0.01	0.26	0.02	0.18	0.07	0.27	0.37	0.51	2.81	–	–	–	–	–	–

Benchmarks

Table: Checking implications between error resistant code formulas (2-safety Hyperproperties).

Ham	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0.03	0.02	0.03	0.02	0.02	0.02	0.03	0.03	0.04	0.08	0.10	0.18	0.25	0.46	0.74	1.35	2.62
1	0.03	0.02	0.03	0.03	0.04	0.03	0.05	0.04	0.06	0.08	0.13	0.21	0.40	0.49	0.82	1.50	2.99
2	0.01	0.03	0.03	0.03	0.04	0.02	0.03	0.04	0.04	0.07	0.12	0.21	0.36	0.55	0.88	1.59	3.09
3	0.03	0.04	0.04	0.05	0.04	0.04	0.03	0.04	0.05	0.07	0.12	0.23	0.36	0.52	0.87	1.56	3.12
4	0.04	0.04	0.04	0.06	0.10	0.02	0.03	0.05	0.08	0.08	0.16	0.21	0.36	0.52	0.86	1.66	3.05
5	0.03	0.03	0.05	0.07	0.07	0.19	0.14	0.17	0.05	0.08	0.14	0.22	0.30	0.52	0.92	1.55	2.99
6	0.03	0.04	0.05	0.06	0.09	0.22	0.35	0.21	0.25	0.11	0.25	0.26	0.36	0.53	0.87	1.57	3.00
7	0.04	0.05	0.05	0.05	0.14	0.24	0.32	0.37	0.38	0.42	0.14	0.20	0.37	0.52	0.89	1.65	3.05
8	0.05	0.05	0.07	0.10	0.17	0.23	0.26	0.36	0.50	0.56	0.47	0.40	0.53	0.53	1.13	1.61	3.18
9	0.07	0.08	0.08	0.10	0.16	0.19	0.21	0.43	0.70	0.64	0.48	0.52	0.90	0.65	1.03	1.71	3.08
10	0.09	0.13	0.15	0.15	0.21	0.20	0.34	0.43	0.54	0.76	1.38	1.55	0.61	0.89	1.03	1.78	3.22
11	0.16	0.23	0.22	0.24	0.24	0.26	0.41	0.53	0.62	0.81	1.30	1.29	1.81	1.05	1.86	2.33	3.17
12	0.27	0.30	0.36	0.30	0.32	0.41	0.45	0.46	0.85	0.91	1.69	1.28	2.81	2.82	1.14	3.91	4.49
13	0.38	0.46	0.51	0.47	0.57	0.52	0.57	0.86	1.03	1.27	1.47	2.16	3.19	8.22	5.48	8.64	7.08
14	0.69	0.87	0.91	0.84	0.84	0.98	0.94	1.02	1.46	1.30	2.01	3.82	3.96	6.35	7.50	9.06	11.11
15	1.22	1.52	1.58	1.70	1.69	1.65	1.67	1.74	1.87	2.73	3.02	3.08	5.87	7.25	13.04	34.17	12.26
16	2.26	3.04	2.97	3.00	3.10	3.11	3.35	3.29	3.57	4.17	3.76	5.78	7.45	17.31	17.75	31.51	48.09

EAHyper

Try EAHyper online: https://www.react.uni-saarland.de/tools/online/EAHyper

Summary

- EAHyper checks the satisfiability, implication, and equivalence of HyperLTL formulas.
- EAHyper can be used to analyze hyperproperties and the relation between different formalizations.
- Code and Benchmarks are available online: https://www.react.uni-saarland.de/tools/eahyper/

Bibliography

[Clarkson, Schneider, ’10] Clarkson, M. R., and F. B. Schneider. "Hyperproperties." Journal of Computer Security 18.6 (2010): 1157-1210.

[Clarkson, Finkbeiner, Koleini, Micinski, Rabe, Sánchez, ’14] Clarkson, M. R., Finkbeiner, B., Koleini, M., Micinski, K. K., Rabe, M. N., & Sánchez, C. (2014, April). Temporal logics for hyperproperties. In International Conference on Principles of Security and Trust (pp. 265-284).

[Finkbeiner, Rabe, Sánchez, ’15] Bernd Finkbeiner, Markus N. Rabe, and César Sánchez. Algorithms for Model Checking HyperLTL and HyperCTL*. International Conference on Computer Aided Verification (2015).

[Finkbeiner, H., ’16] Finkbeiner, Bernd, Hahn, Christopher. Deciding hyperproperties. 27th International Conference on Concurrency Theory, CONCUR 2016