Towards Using Multiple Counterexamples for Abstraction Refinement

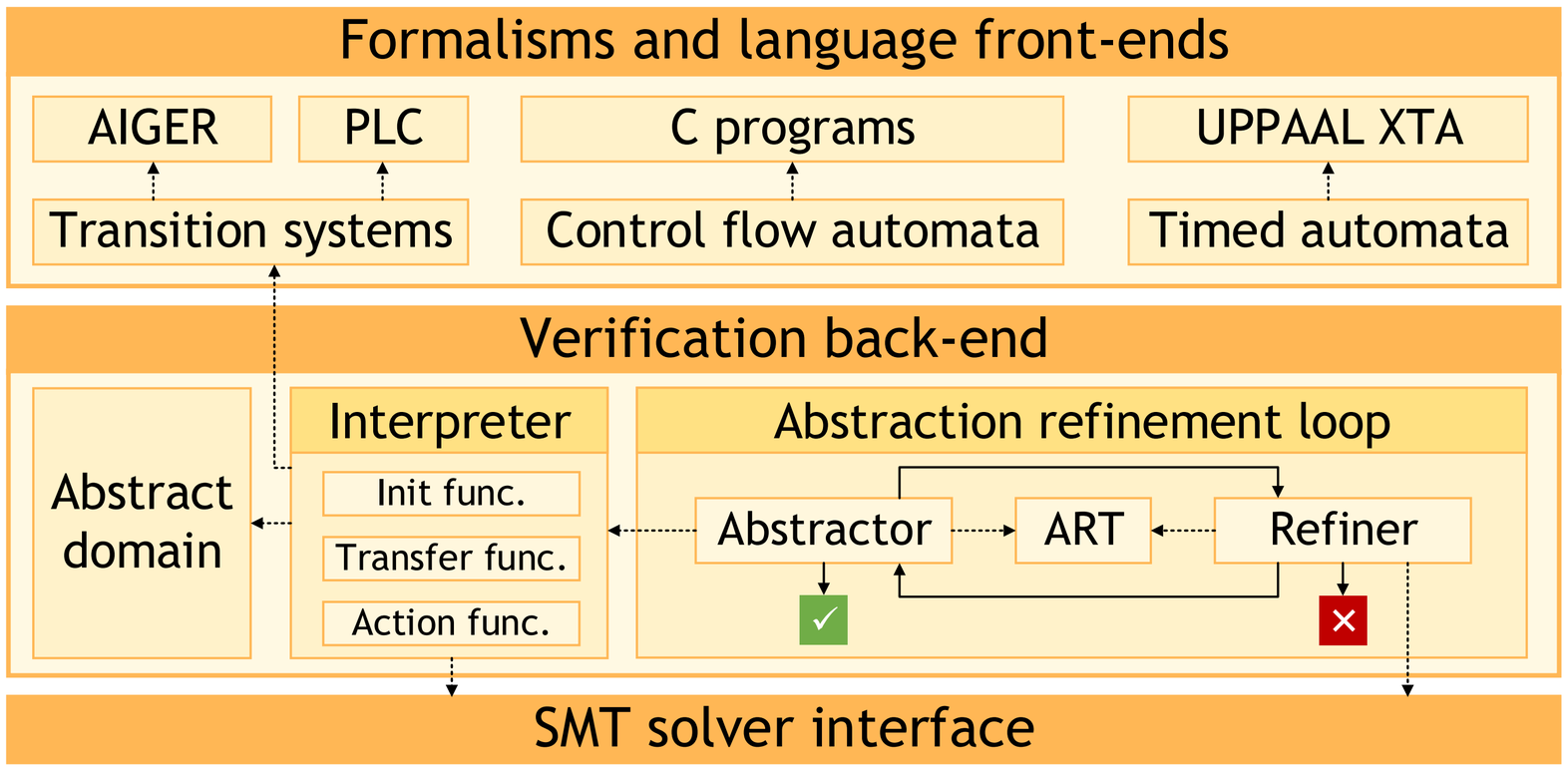
Ákos Hajdu, Zoltán Micskei

Context

Theta Framework

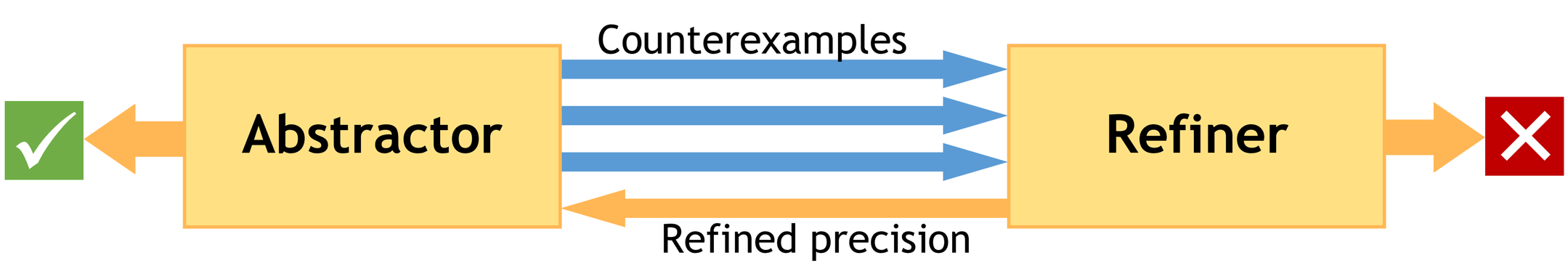
- Framework for abstraction refinement-based algorithms
- Generic, modular, configurable
- Easy development, evaluation and combination of algorithms
- Support for various formalisms
- Applicable for systems with different aspects (e.g. CPS)
- Open source
  github.com/FTSRG/theta

Architecture



Research Question

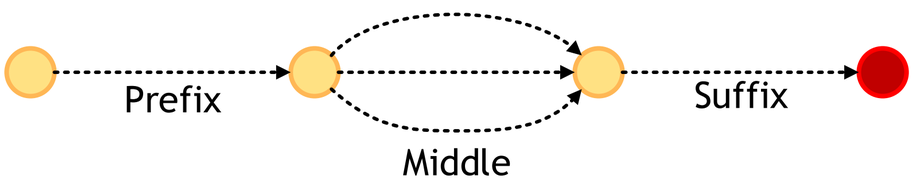
Considering multiple counterexamples for abstraction refinement:
overhead ↔ better refinements (?)



Preliminary Results

Experiments on SV-COMP, HWMCC, PLC models identified two kinds of counterexample structures

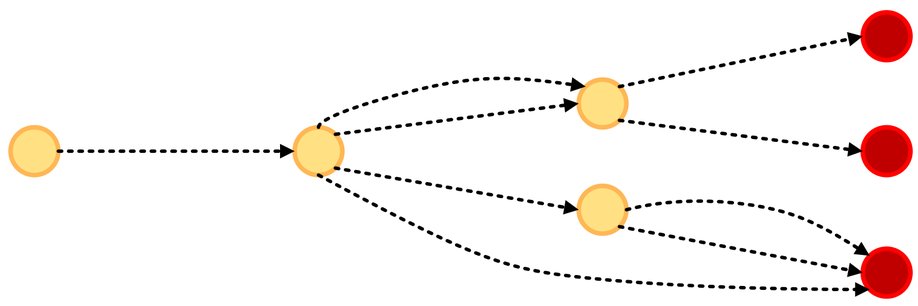
Multiple paths, single erroneous state



Refinement ideas

- Prune path in prefix/suffix: no benefit
- Prune path in middle: eliminate all counterexamples in a single iteration
  - Fewer but larger iterations
  - Explore *k* counterexamples → configurable

Multiple paths, multiple erroneous states



Refinement ideas

- Prefer strategy that prunes closest to the initial state
- Calculate refinement for each path and determine (coarsest) common precision eliminating all counterexamples

Budapest University of Technology and Economics
Fault Tolerant Systems Research Group
http://inf.mit.bme.hu/en

MŰEGYETEM 1782