UNIVERSITY OF CAMBRIDGE

Hoare Logic and Model Checking – additional slide

Alan Mycroft

May 21, 2018

Generating counterexamples (explicit states)

Can use 'failure to prove' to generate counter-example traces.

Here 'trace' is a synonym for 'path'

Easy, but potentially slow using explicit state representation:

- Suppose not all reachable states of model M satisfy p
- i.e. $\exists s \in \text{Reachable } M.\ \neg p(s)$
- Set of reachable states $\mathcal{S}$ given by: $\mathcal{S} = \bigcup_{n=0}^{\infty} \mathcal{S}_n$
- Iterate to find least n such that $\exists s \in \mathcal{S}_n.\ \neg p(s)$ (helpful to report the the shortest error trace)
- Pick a state s_n such that $s_n \in \mathcal{S}_n \wedge \neg p(s_n)$
- Find a path $s_0 \in S_0 \ldots s_n \in \mathcal{S}_n$ to it

Finding a path in (S, S_0, R, L) is linear time if we store breadcrumbs (back-pointers from each reachable state s_{i+1} to the state s_i which first caused it to be visited); s_0 is necessarily part of $S_0 = \mathcal{S}_0$