ECE/CS 584: PVS Tutorial Part 1

Lecture 05

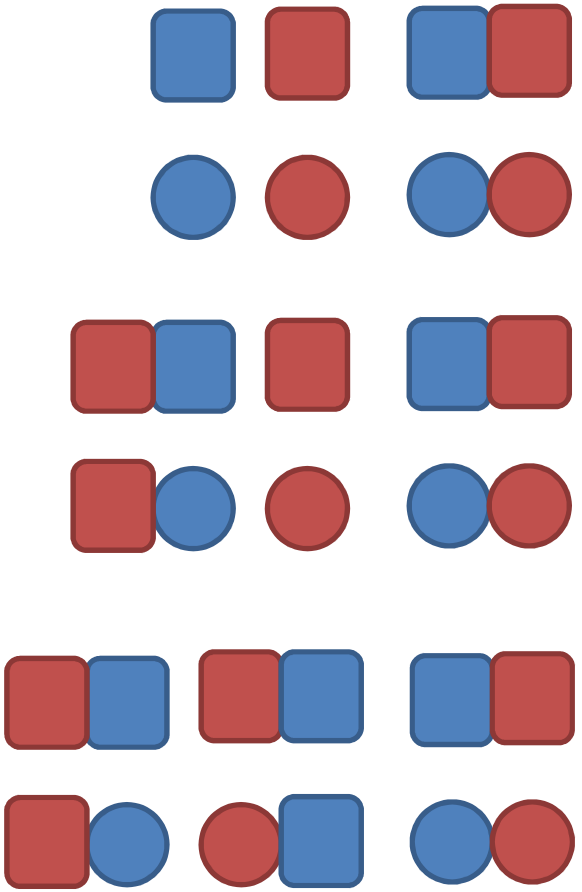
Sayan Mitra

Plan for Today

- Substitutivity final comments
- PVS tutorial Part 1

Recap

- Composition $\mathcal{A}_1 \,||\, \mathcal{A}_2$
- α execution fragment of $\boldsymbol{\mathcal{A}}$ iff $\alpha_i = \alpha\lceil(A_i, X_i)$ is an execution fragment of $\mathcal{A}_i$
- $\text{Traces}_{\mathcal{A}} = \{\, \beta \mid \beta\lceil E_i \in \text{Traces}\, \mathcal{A}_i \,\}$
- **Theorem 1.** If $\mathcal{A}_1 \leq \mathcal{A}_2$ and $\mathcal{B}_1 \leq \mathcal{B}_2$
  then $\mathcal{A}_1 \,||\, \mathcal{B}_1 \leq \mathcal{A}_2 \,||\, \mathcal{B}_2$.
- **Theorem 2.** If $\mathcal{A}_1 \,||\, \mathcal{B}_2 \leq \mathcal{A}_2 \,||\, \mathcal{B}_2$ and $\mathcal{B}_1 \leq \mathcal{B}_2$
  then $\mathcal{A}_1 \,||\, \mathcal{B}_1 \leq \mathcal{A}_2 \,||\, \mathcal{B}_2$.
- **Conjecture.** If $\mathcal{A}_1 \,||\, \mathcal{B}_2 \leq \mathcal{A}_2 \,||\, \mathcal{B}_2$ & $\mathcal{A}_2 \,||\, \mathcal{B}_1 \leq \mathcal{A}_2 \,||\, \mathcal{B}_2$
  then $\mathcal{A}_1 \,||\, \mathcal{B}_1 \leq \mathcal{A}_2 \,||\, \mathcal{B}_2$?



Fun with compositions

- 4 automata, all have the same external actions a, b

automaton CatchUpA

- external a, b
- states counta : Nat := 0, countb : Nat := 0, now : Real := 0, next : di screte Real := 0
- transitions

  external a

  pre (counta ≤ countb) /\ (now = next)

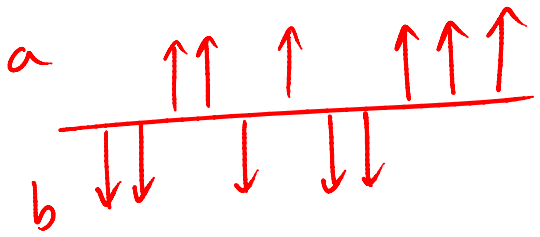
  eff counta := counta + 1; next := now + 1

  external b

  eff countb := countb + 1; next := now + 1
- trajectories

  stop when now = next

  evolve d(now) = 1



automaton CatchUpB

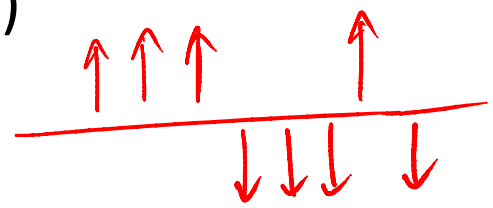
- external a, b
- states counta : Nat := 0, countb : Nat := 0, now : Real := 0, next : di screte Real := 0
- transitions
- external b
- pre (countb + 1 ≤ counta) /\ (now = next)

  eff countb := countb + 1; next := now + 1
- external a

  eff counta := counta + 1; next := now + 1
- trajectories

  stop when now = next

  evolve d(now) = 1



- CatchUpA can perform arbitrarily many b's and an a if counta $\leq$countb
- CatchUpB can perform arbitrarily many a's and a b if counta $<$countb
- CatchUpA || CatchUpB can perform arbitrarily many a's and b's

automaton BoundedAlternateA

external a, b

states myturn : Bool := true, maxout : Nat

transitions

- external b

  eff myturn := true

- external a

  pre myturn /\ (maxout > 0)

  eff myturn := false ; maxout := maxout - 1

automaton BoundedAlternateB

external a, b

states myturn : Bool := false, maxout : Nat

transitions

- external a

  eff myturn := true

- external b

  pre myturn /\ (maxout > 0)

  eff myturn := false ; maxout := maxout - 1

Putting it all together

- For a given value of maxout BoundedAlternateA performs a finite number of a's and arbitrarily many b's
- CatchUpA || BoundedAlternateB performs a finite number of alternating A's and B's
- BoundedAlternateA || BoundedAlternateB performs a finite number of alternating A's and B's
- CatchUpA||BoundedAlternateB $\leq$ BoundedAlternateA ||BoundedAlternateB
- CatchUpB||BoundedAlternateA $\leq$ BoundedAlternateB ||BoundedAlternateA
- But
- CatchUpA || CatchUpB $\not\leq$ BoundedAlternateA ||BoundedAlternateB

Wrap-up for Hybrid Automaton Modeling Framework

- Nondeterministic state machines
- Abstract transitions and trajectories
- Synchronization through shared actions
  - Shared variables (used Hybrid I/O automata)
- Executions, Reachability, Traces
- Forward backward simulations
- Substitutivity