# LoopInvGen:

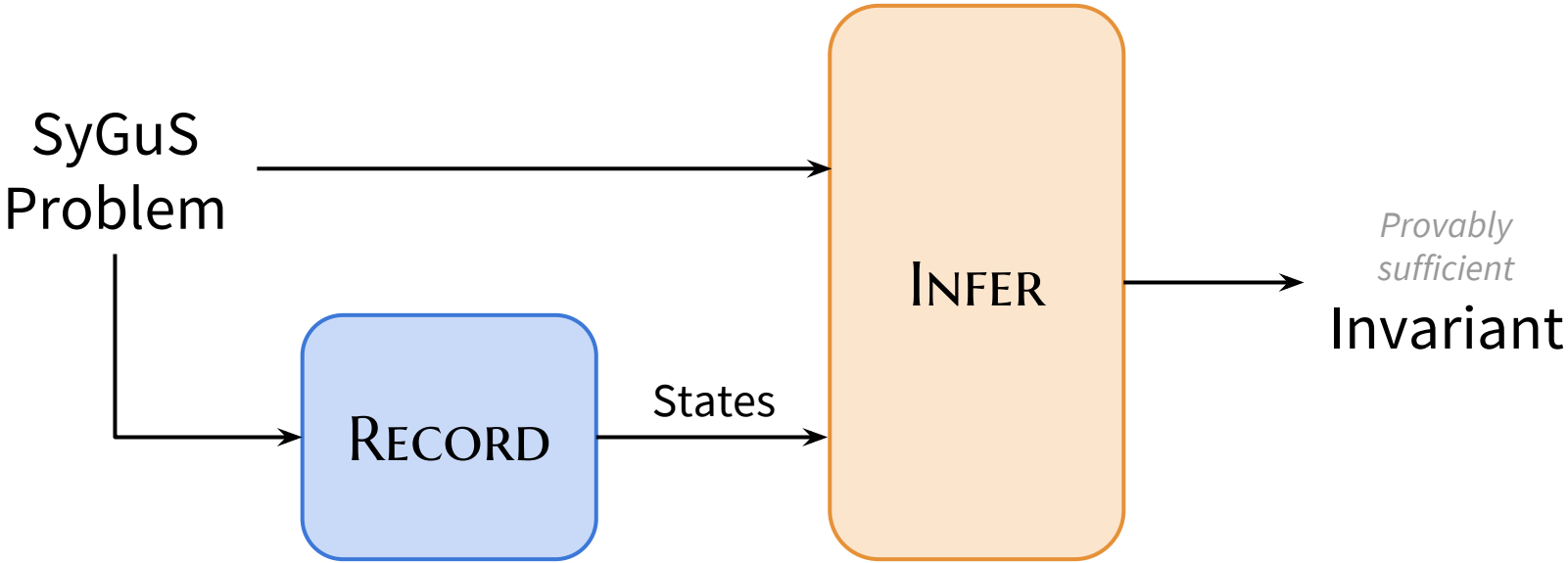
# Data-Driven Loop Invariant Inference using Learned Features

*SyGuS-COMP 2017*

Saswat Padhi Todd Millstein

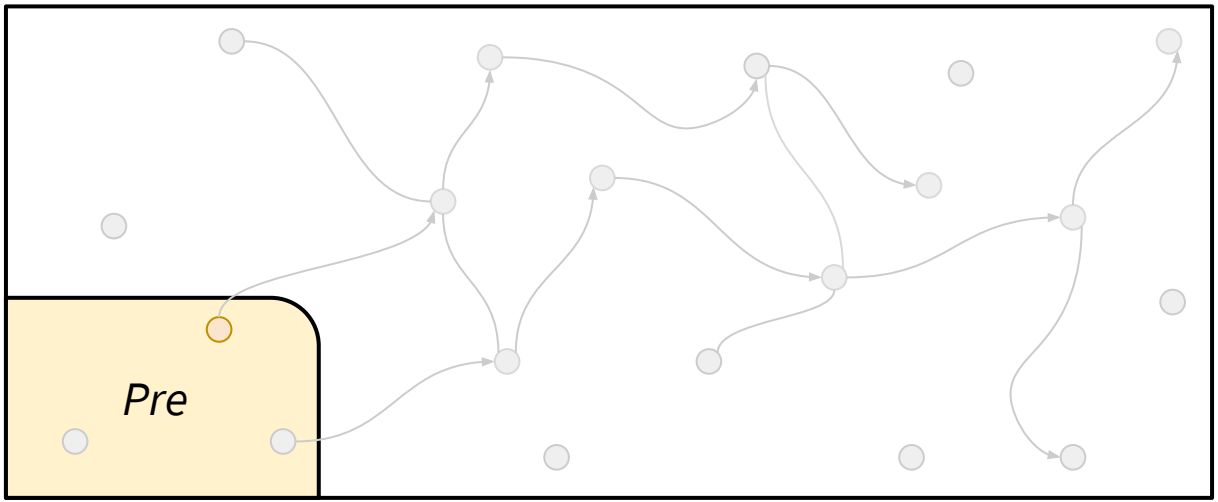
(University of California, Los Angeles)

# Overview


SyGuS
Problem
Record
States
Infer
Provably
sufficient
Invariant

# RECORD-ing Reachable States

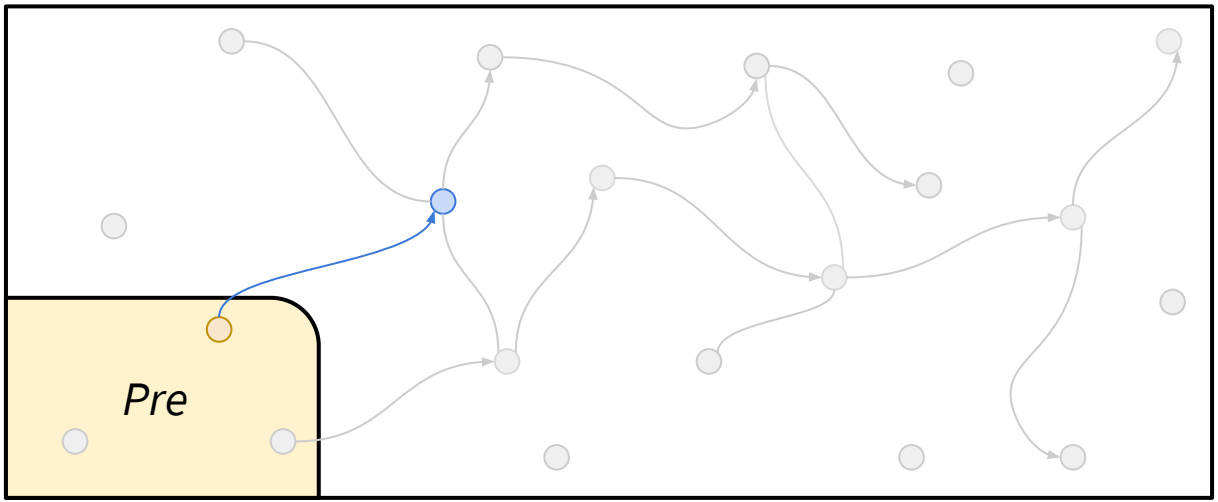
SyGuS Problem (Pre, Trans, Post) →List of variable assignments




1. Pick state s, s.t. Pre(s)

# RECORD-ing Reachable States

SyGuS Problem (Pre, Trans, Post) →List of variable assignments

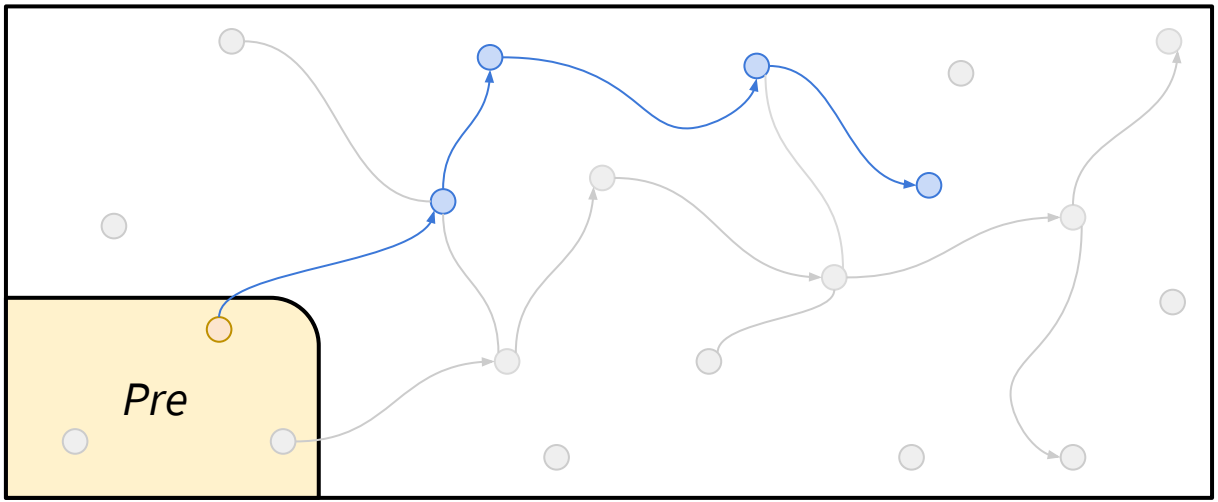



1. Pick state s, s.t. Pre(s)

2. Obtain state t, s.t. Trans(s,t)

# RECORD-ing Reachable States

SyGuS Problem (Pre, Trans, Post) →List of variable assignments



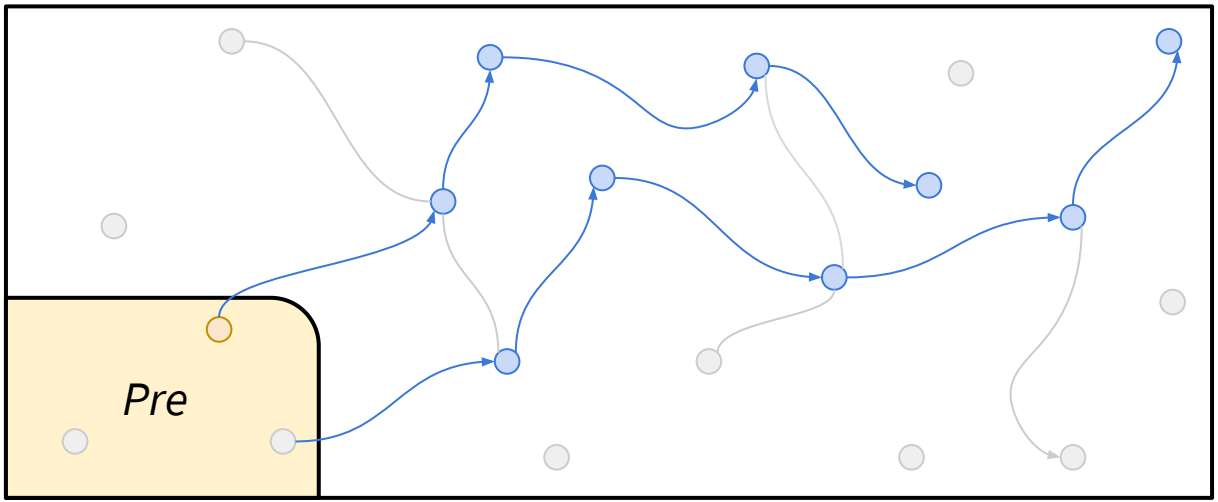

1. Pick state s, s.t. Pre(s)

2. Obtain state t, s.t. Trans(s,t)

3. Set s ← t and repeat (2)

# RECORD-ing Reachable States

SyGuS Problem (Pre, Trans, Post) →List of variable assignments

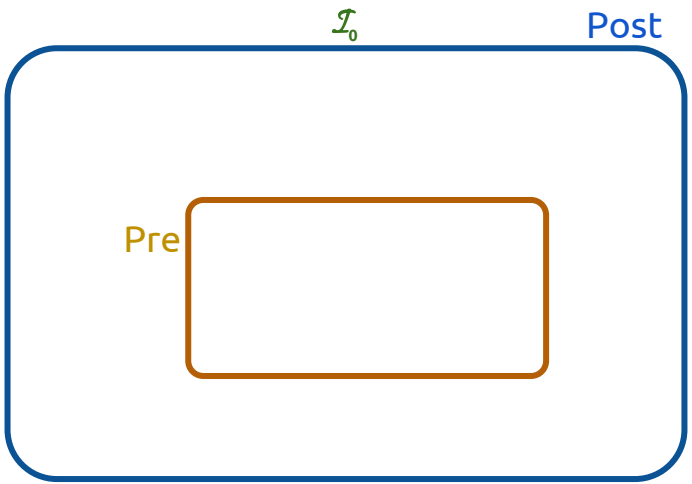



1. Pick state s, s.t. Pre(s)  2. Obtain state t, s.t. Trans(s,t)  3. Set s ← t and repeat (2)

4. Repeat (1,2,3) till the desired number of states has been collected

# INFER-ing Sufficient Invariants

- ∀ s: Pre(s) ⇒ $\mathcal{I}$(s)
- ∀ s, t: $\mathcal{I}$(s) ∧ Trans(s,t) ⇒ $\mathcal{I}$(t)
- ∀ s: $\mathcal{I}$(s) ⇒ Post(s)

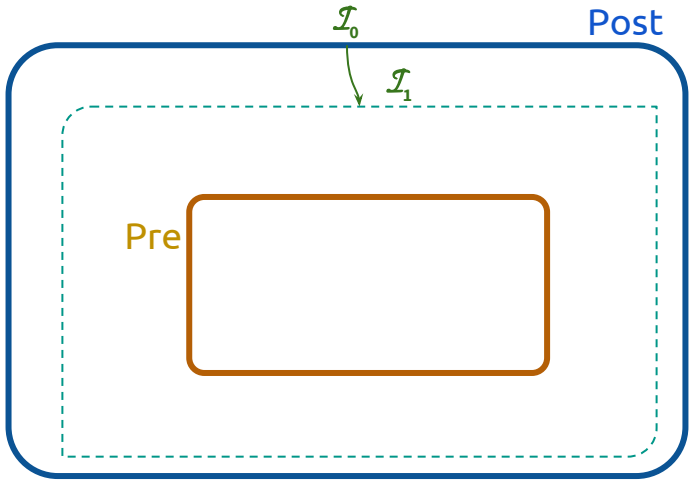



1. Start with the weakest candidate

$\mathcal{I}_0$ = Post

# INFER-ing Sufficient Invariants

- ∀ s: Pre(s) ⇒ $\mathcal{I}$(s)
- ∀ s,t: $\mathcal{I}$(s) ∧ Trans(s,t) ⇒ $\mathcal{I}$(t)
- ∀ s: $\mathcal{I}$(s) ⇒ Post(s)




1. Start with the weakest candidate
2. Iteratively <u>strengthen</u> for inductiveness (by using precondition inference)

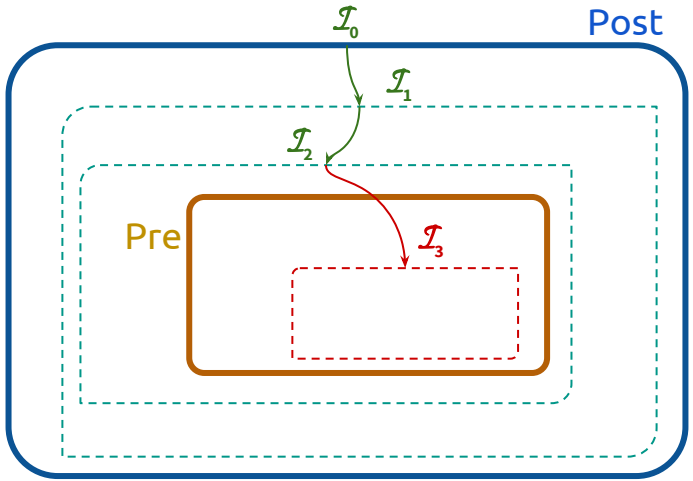
$\mathcal{I}_0$ = Post

$\delta_0 \Rightarrow (\mathcal{I}_0 \wedge \text{Trans} \Rightarrow \mathcal{I}_0')$

$\mathcal{I}_1 = \delta_0 \wedge \mathcal{I}_0$

# INFER-ing Sufficient Invariants

- ∀ s: Pre(s) ⇒ $\mathcal{I}$(s)
- ∀ s, t: $\mathcal{I}$(s) ∧ Trans(s,t) ⇒ $\mathcal{I}$(t)
- ∀ s: $\mathcal{I}$(s) ⇒ Post(s)




1. Start with the weakest candidate
2. Iteratively <u>strengthen</u> for inductiveness (by using precondition inference)

$\mathcal{I}_0$ = Post

$\delta_0 \Rightarrow (\mathcal{I}_0 \wedge \text{Trans} \Rightarrow \mathcal{I}_0')$

$\mathcal{I}_1 = \delta_0 \wedge \mathcal{I}_0$

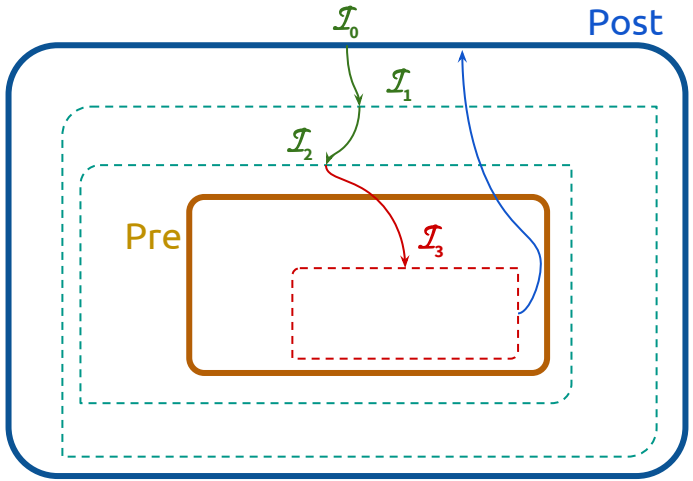
$\delta_1 \Rightarrow (\mathcal{I}_1 \wedge \text{Trans} \Rightarrow \mathcal{I}_1')$

⋮ ⋮ ⋮ ⋮

# INFER-ing Sufficient Invariants

- ∀ s: Pre(s) ⇒ $\mathcal{I}$(s)
- ∀ s, t: $\mathcal{I}$(s) ∧ Trans(s,t) ⇒ $\mathcal{I}$(t)
- ∀ s: $\mathcal{I}$(s) ⇒ Post(s)

1. Start with the weakest candidate
2. Iteratively strengthen for inductiveness (by using precondition inference)
3. If the invariant is too strong, restart from (1) after augmenting the recorded states with appropriate counterexamples




$\mathcal{I}_0$ = Post

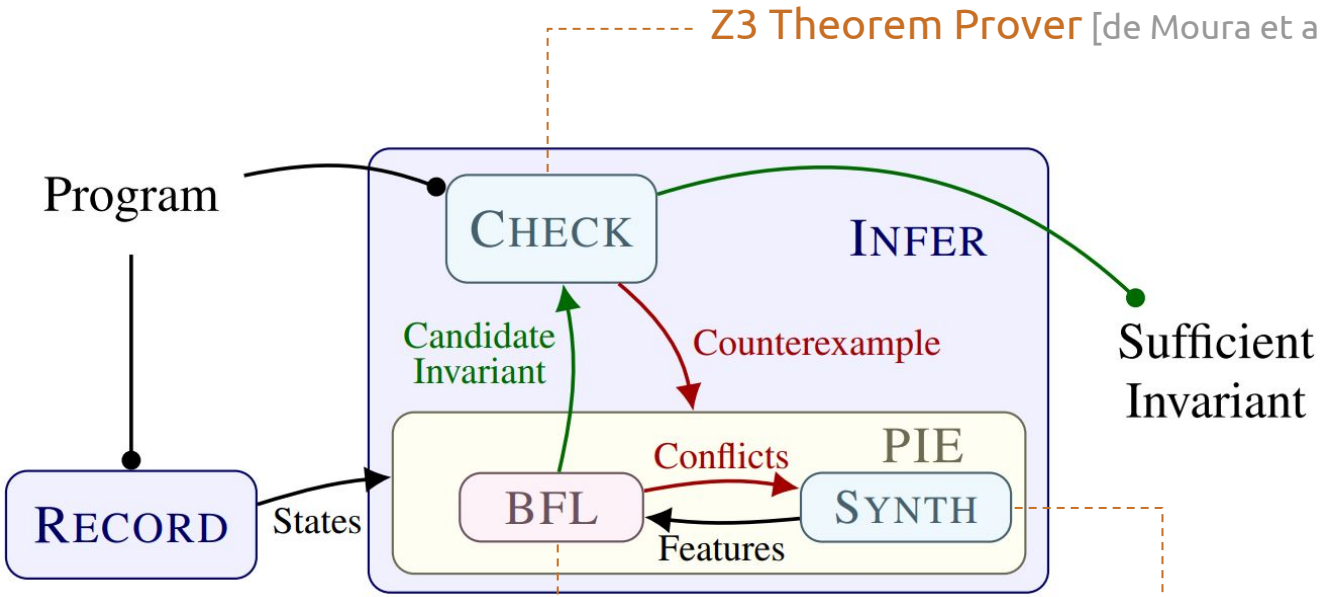
$\delta_0 \Rightarrow (\mathcal{I}_0 \wedge \text{Trans} \Rightarrow \mathcal{I}_0')$

$\mathcal{I}_1 = \delta_0 \wedge \mathcal{I}_0$

$\delta_1 \Rightarrow (\mathcal{I}_1 \wedge \text{Trans} \Rightarrow \mathcal{I}_1')$

⋮ ⋮ ⋮ ⋮

# LoopInvGen Architecture



# Thanks! ☺

Reach us at:

padhi @ cs . ucla . edu