DVLAB

Adaptive Interpolation-Based Model Checking

Chien-Yu (Leo) Lai, Cheng-Yin Wu,

Chun-Yang (Ric) Huang

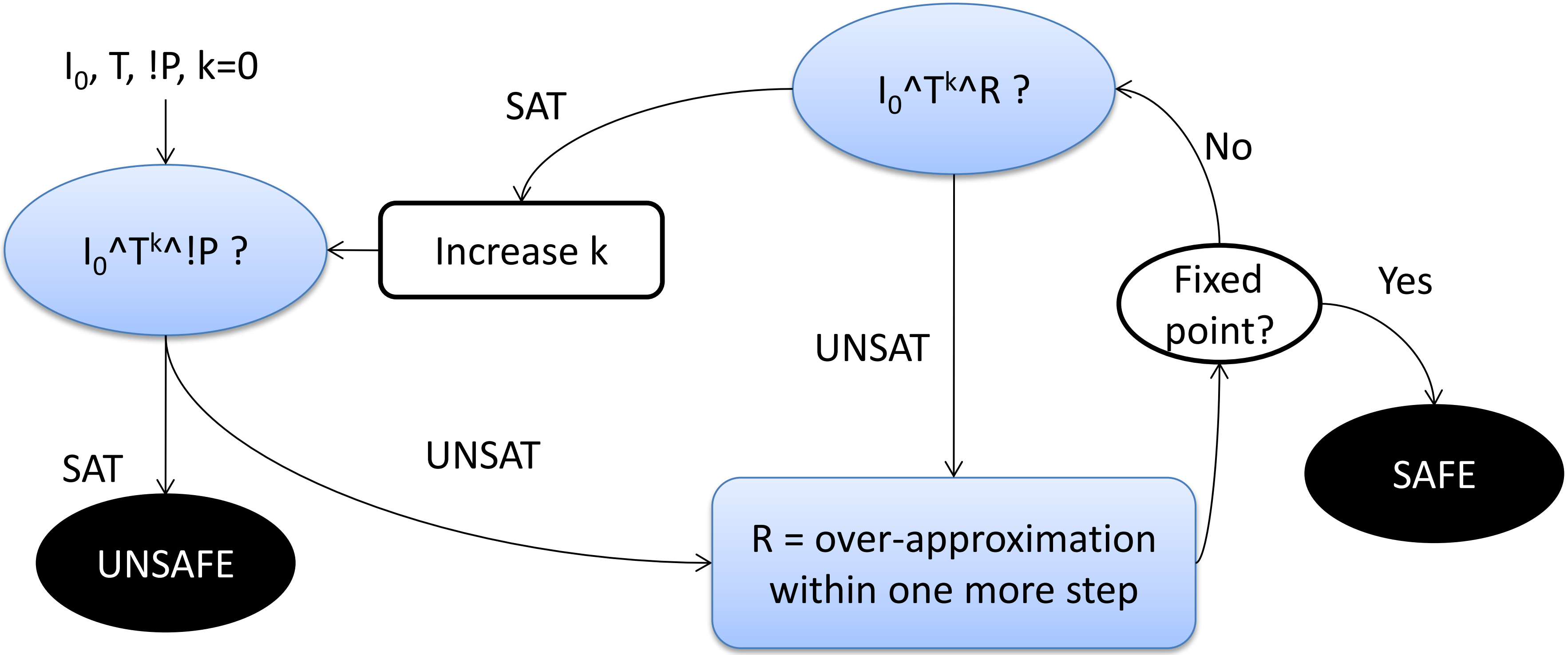
2014.1.23

Outline

- Introduction
- Adaptive IMC Framework
- Flexible Interpolation
- Experimental Results
- Conclusion

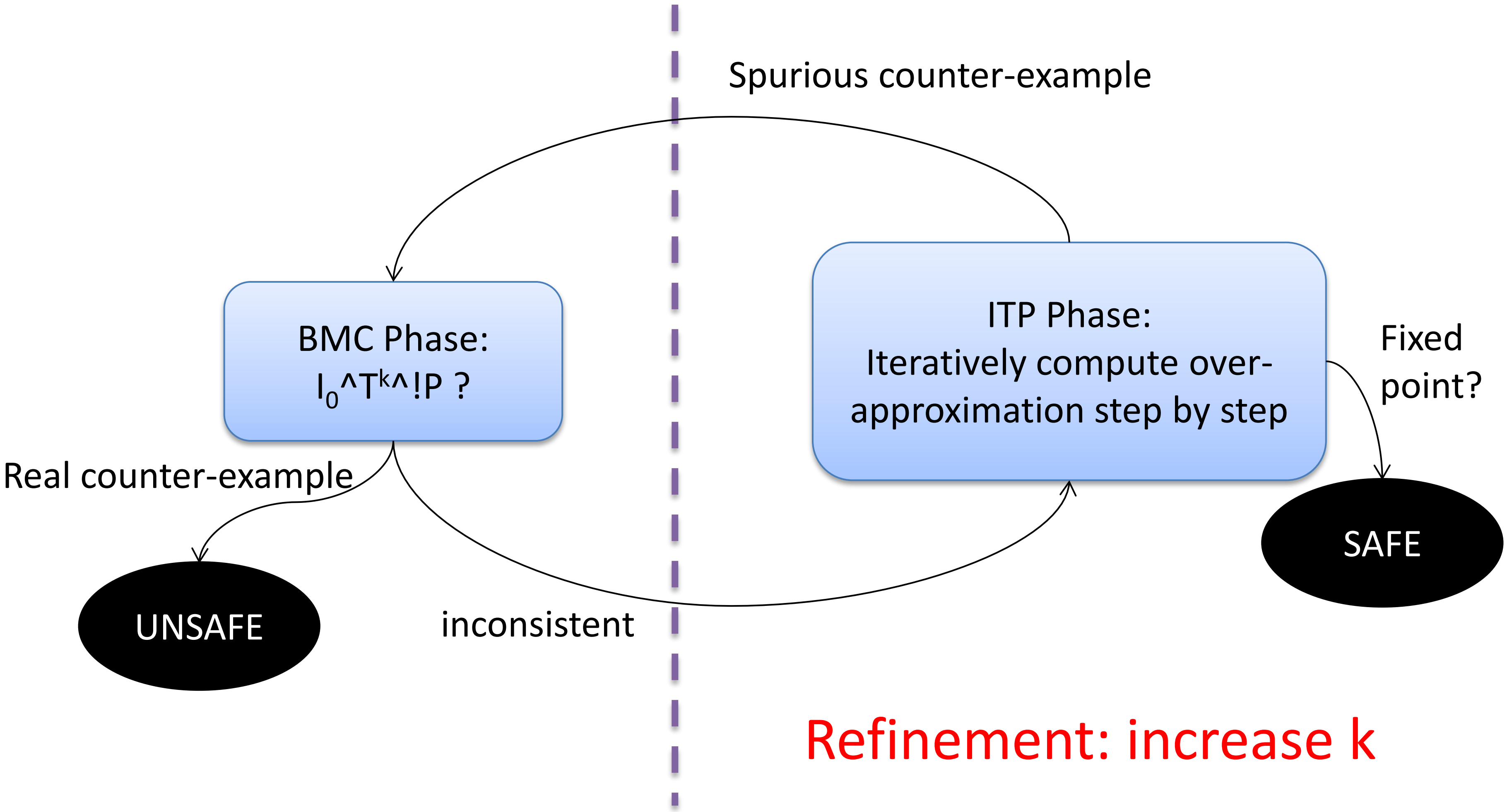
INTRODUCTION

Interpolation-Based Model Checking (IMC)[1]



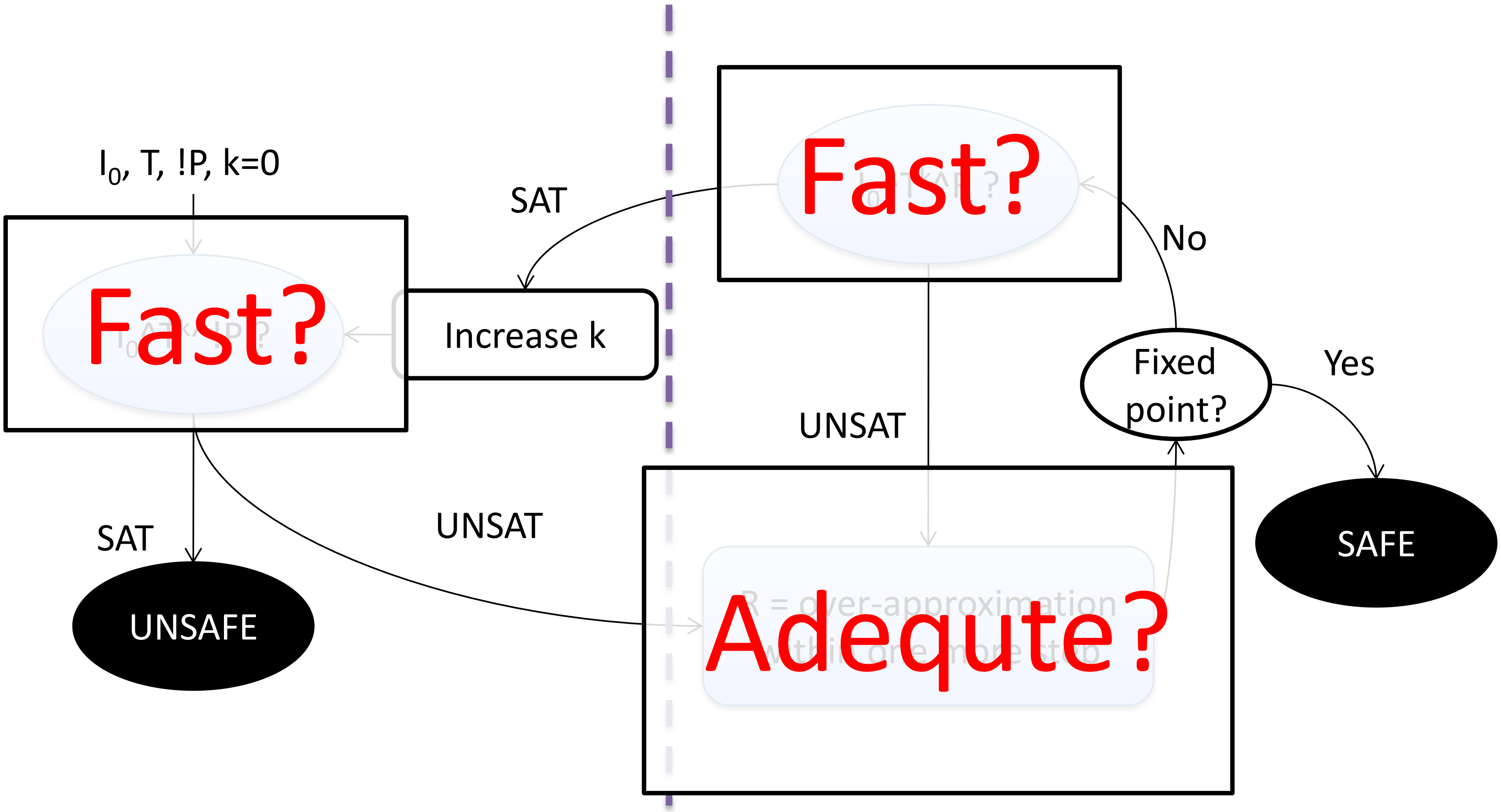
[1] K. L. McMillan, Interpolation and SAT-based model checking (CAV 2003)

Interpolation-Based Model Checking (IMC)



Refinement: increase k

Interpolation-Based Model Checking (IMC)



I_0, T, !P, k=0

$I_0 \wedge T^k \wedge !P$?

Fast?

SAT

UNSAT

UNSAFE

Increase k

SAT

$I_0 \wedge T \wedge F$?

Fast?

UNSAT

R = over-approximation within one more step

Adequte?

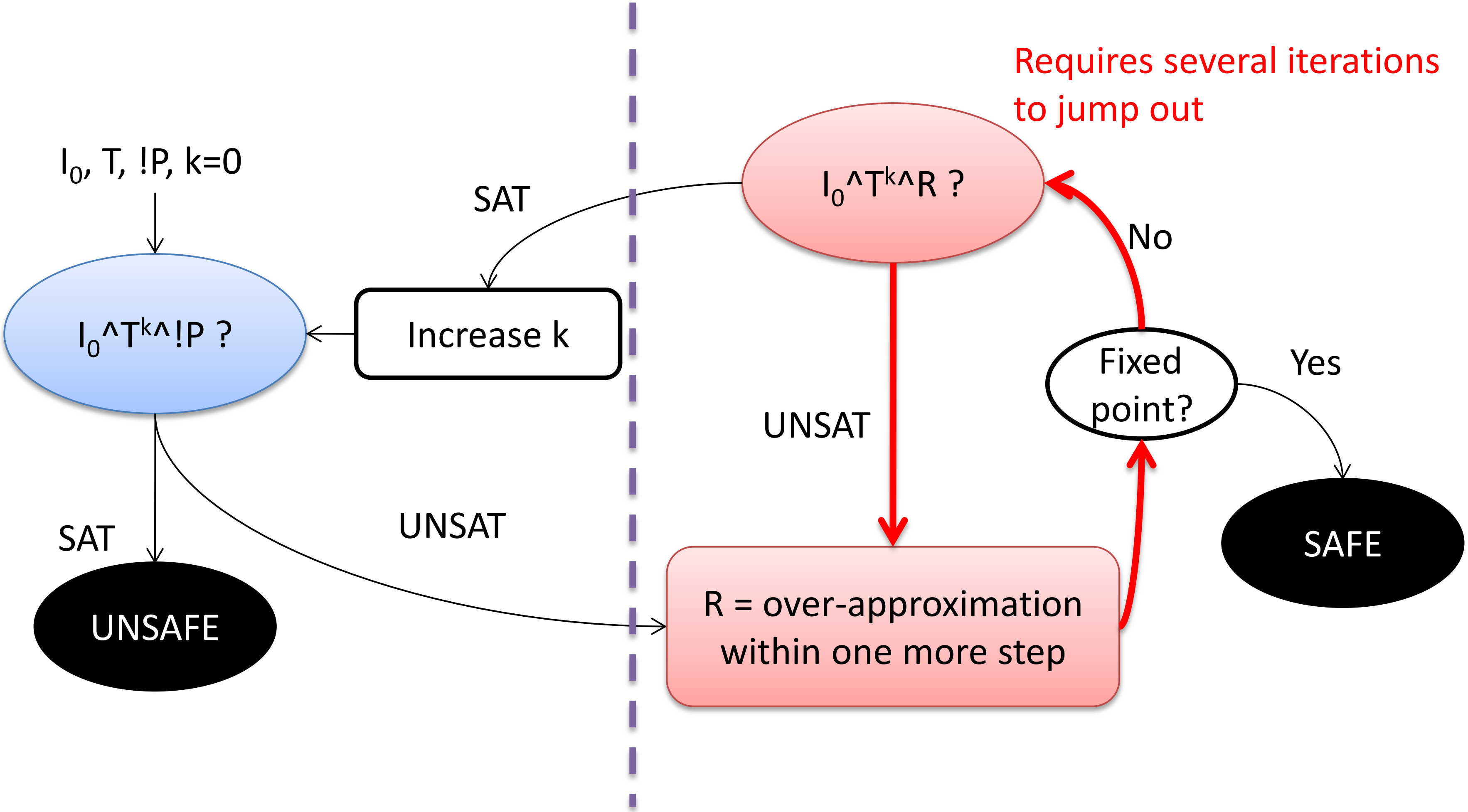
No

Fixed point?

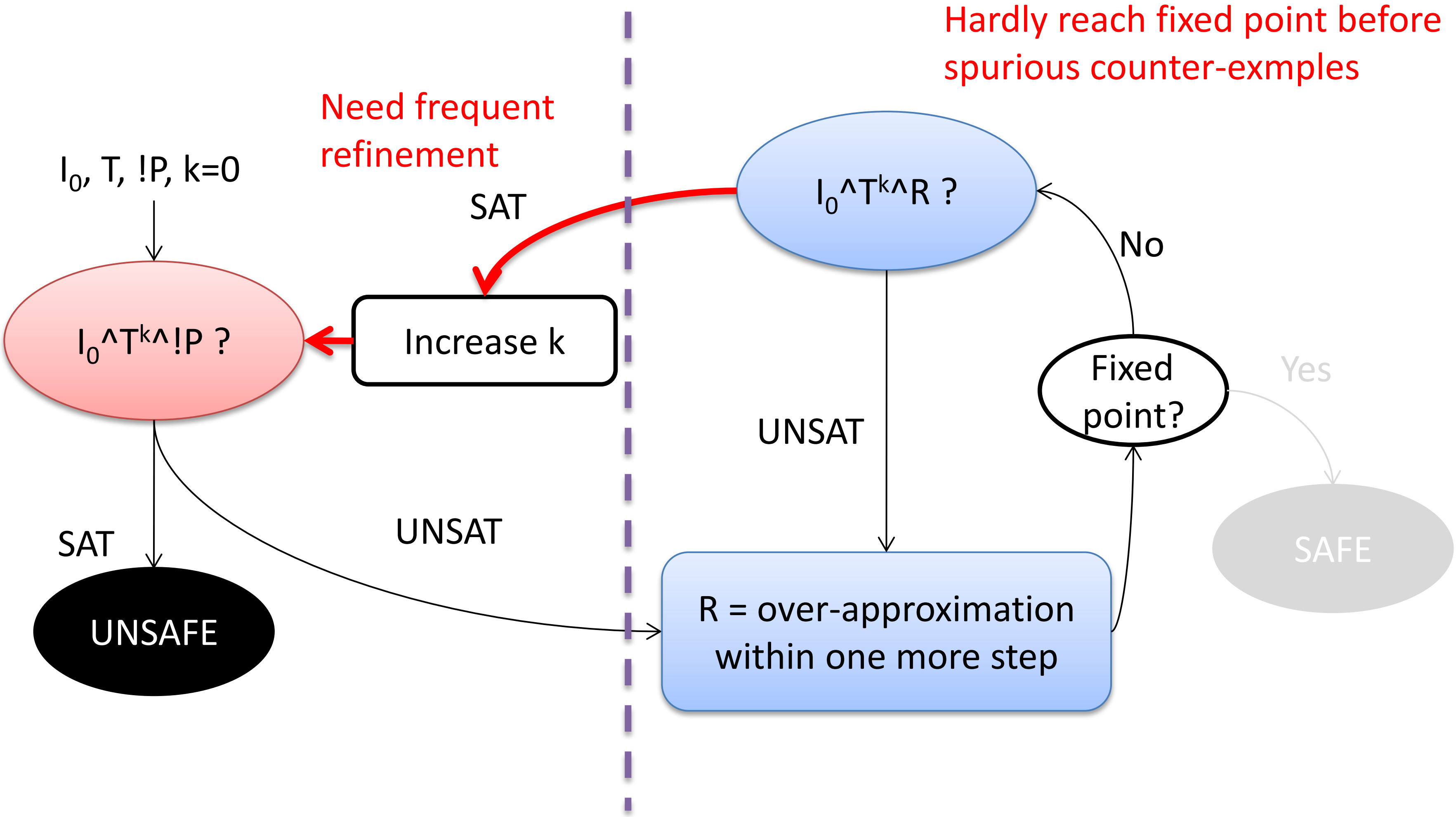
Yes

SAFE

Too fine-grained

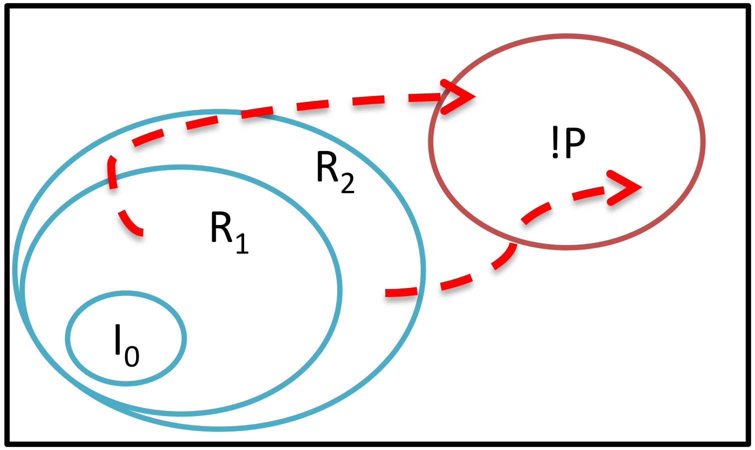


Too Coarse

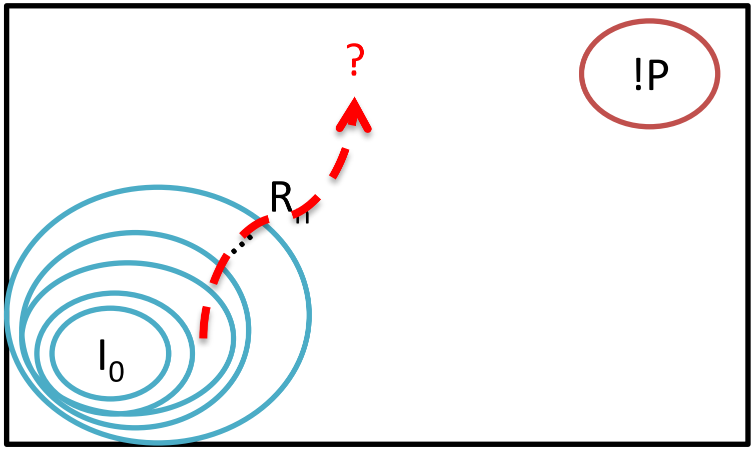


Need frequent refinement
Hardly reach fixed point before spurious counter-exmples
I_0, T, !P, k=0
I_0^T^k^!P ?
SAT
UNSAFE
UNSAT
Increase k
SAT
I_0^T^k^R ?
UNSAT
R = over-approximation within one more step
Fixed point?
No
Yes
SAFE

Two examples



Need for finer-grained abstraction



Need for coarser abstraction

⇢ Spurious counter-example

○ Abstract reachability

○ Bad states

Previous Works – Single, Blind Granularities

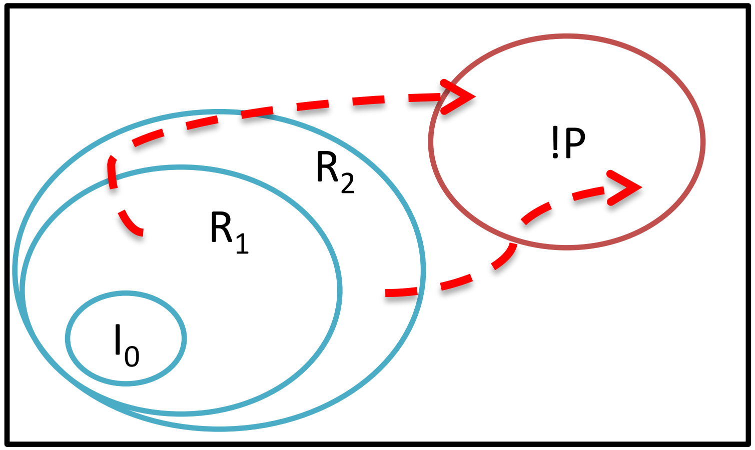
- McMillan's IMC[1]
  - – Depends only on the refutation proof
- NewITP[2]
  - – Depends only on the strength of SAT/UNSAT generalizations

[1] K. L. McMillan, Interpolation and SAT-based model checking (CAV 2003)

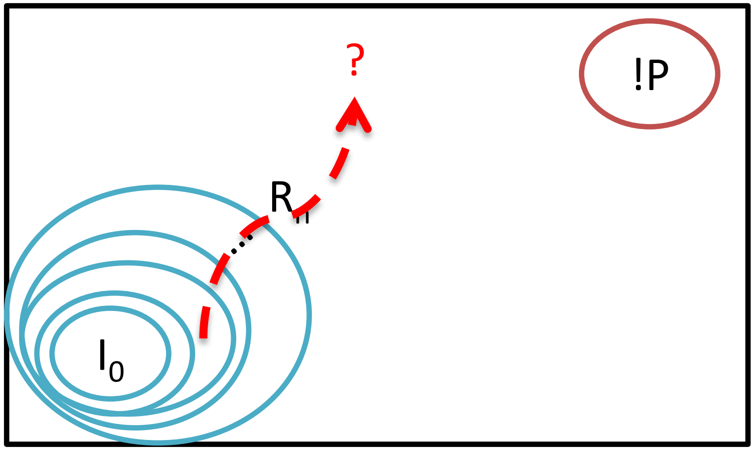
[2] C.Y. Wu, A counterexample-guided interpolant generation algorithm for SAT-based model checking (DAC'13)

Two examples (review)

With single granularity, IMC hardly solves both of them



Need for finer-grained abstraction



Need for coarser abstraction

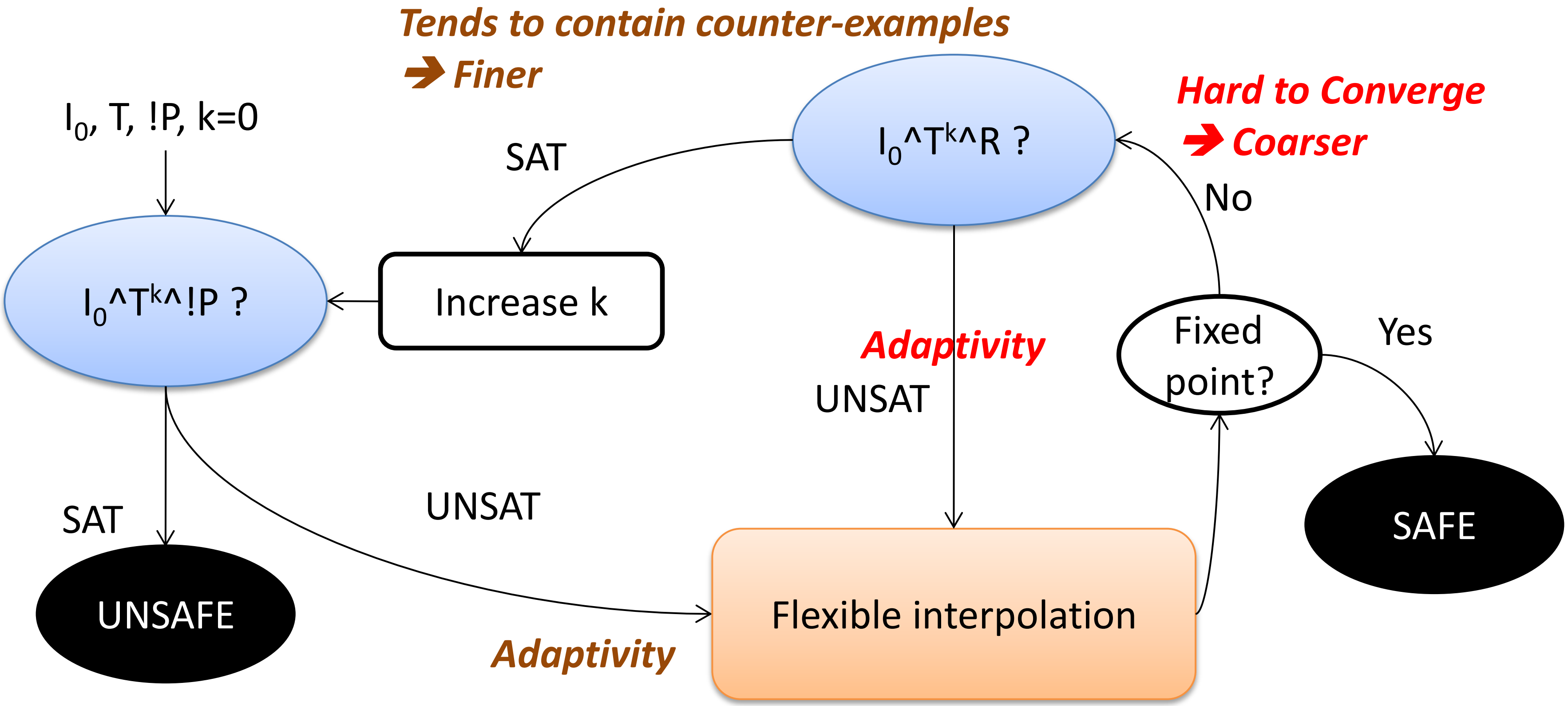
⇢ Spurious counter-example

◯ Abstract reachability

◯ Bad states

ADAPTIVE IMC FRAMEWORK

Adaptive IMC Framework



Tends to contain counter-examples

➔ *Finer*

I_0, T, !P, k=0

SAT

I_0^T^k^R ?

Hard to Converge

➔ *Coarser*

No

I_0^T^k^!P ?

Increase k

Fixed point?

Yes

Adaptivity

UNSAT

SAFE

SAT

UNSAT

UNSAFE

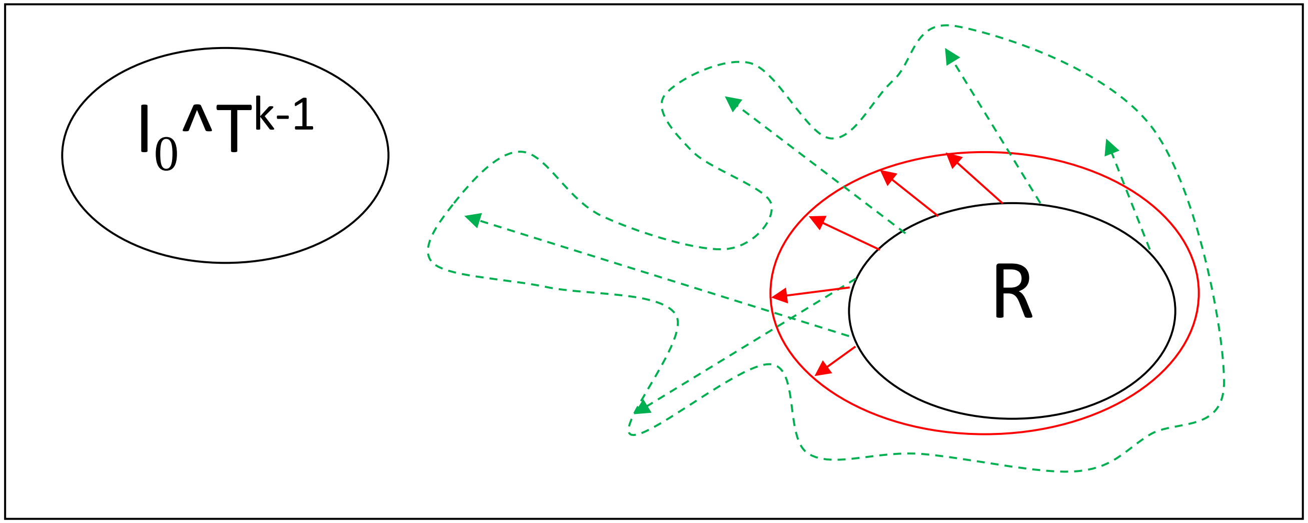
Flexible interpolation

Adaptivity

FLEXIBLE INTERPOLATION BY REACHABILITY PARTITIONING

Reachability v.s. Granularity

- When I_0^T^{k-1}^T^R is UNSAT, not all clauses get involved with UNSAT proof

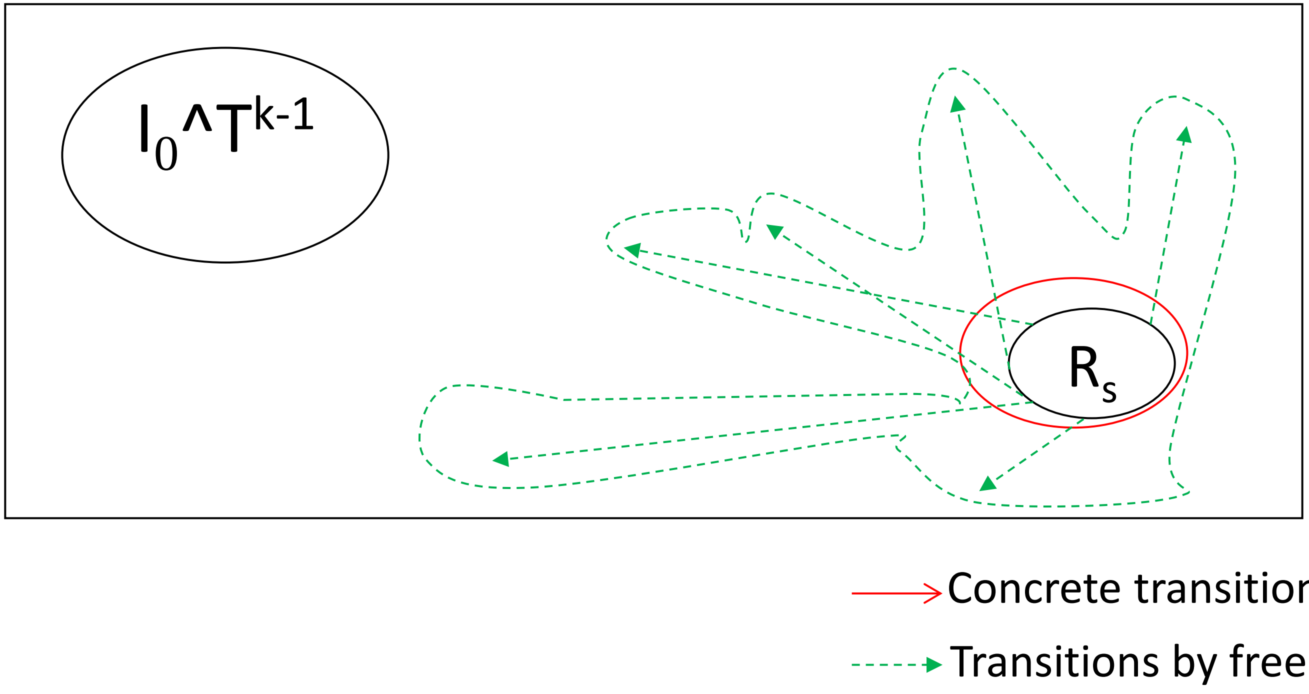


→ Concrete transitions

⇢ Transitions by freed constrains

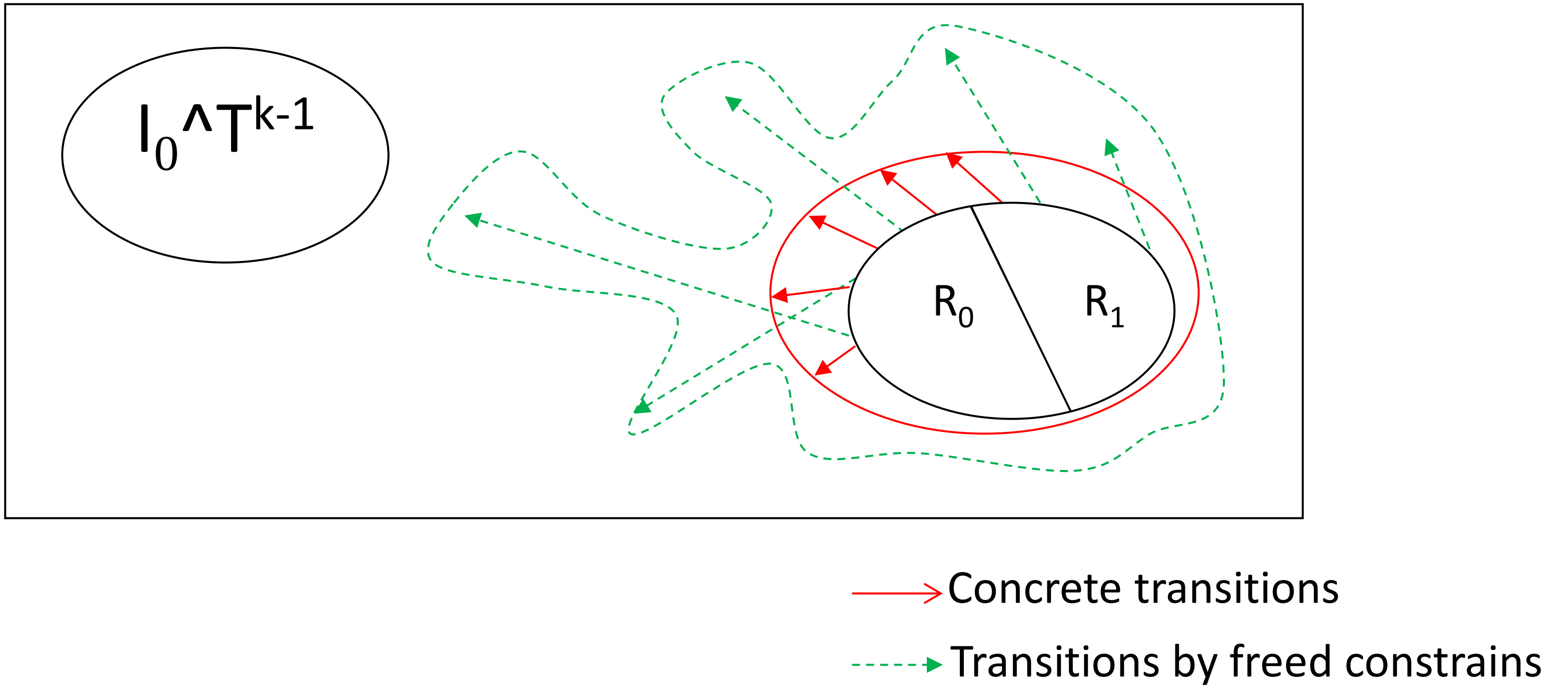
Reachability v.s. Granularity

- If the reachability is smaller, more clauses are absent in UNSAT proof



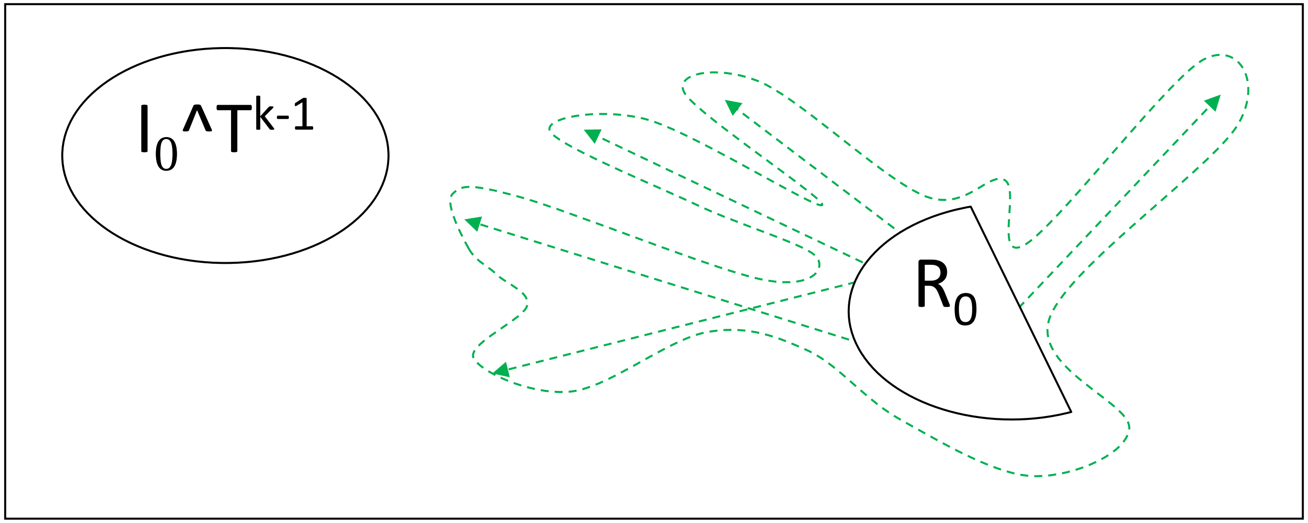
Make Abstraction Coarse

- By just partitioning R into 2 slices



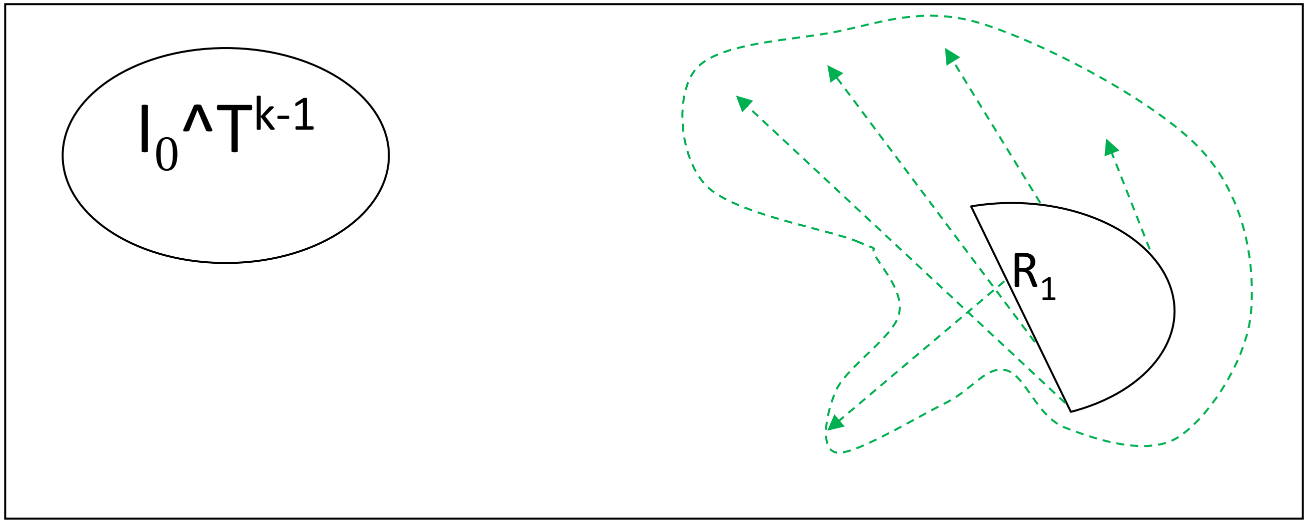
Make Abstraction Coarse

- Constrains restricting the transitions from R_1 is missing



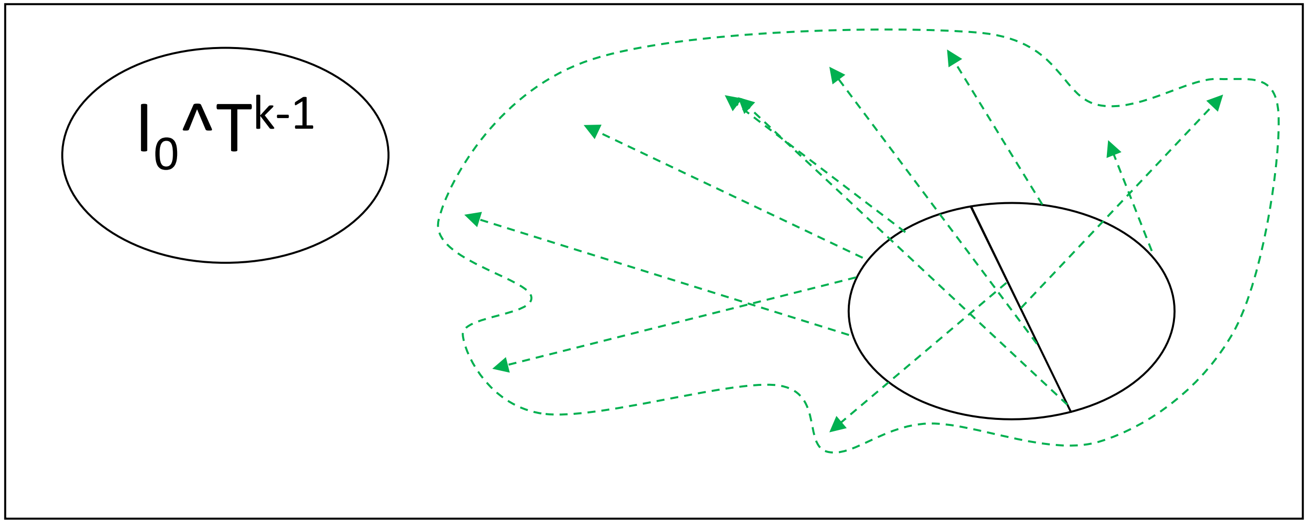
Make Abstraction Coarse

- Likewise

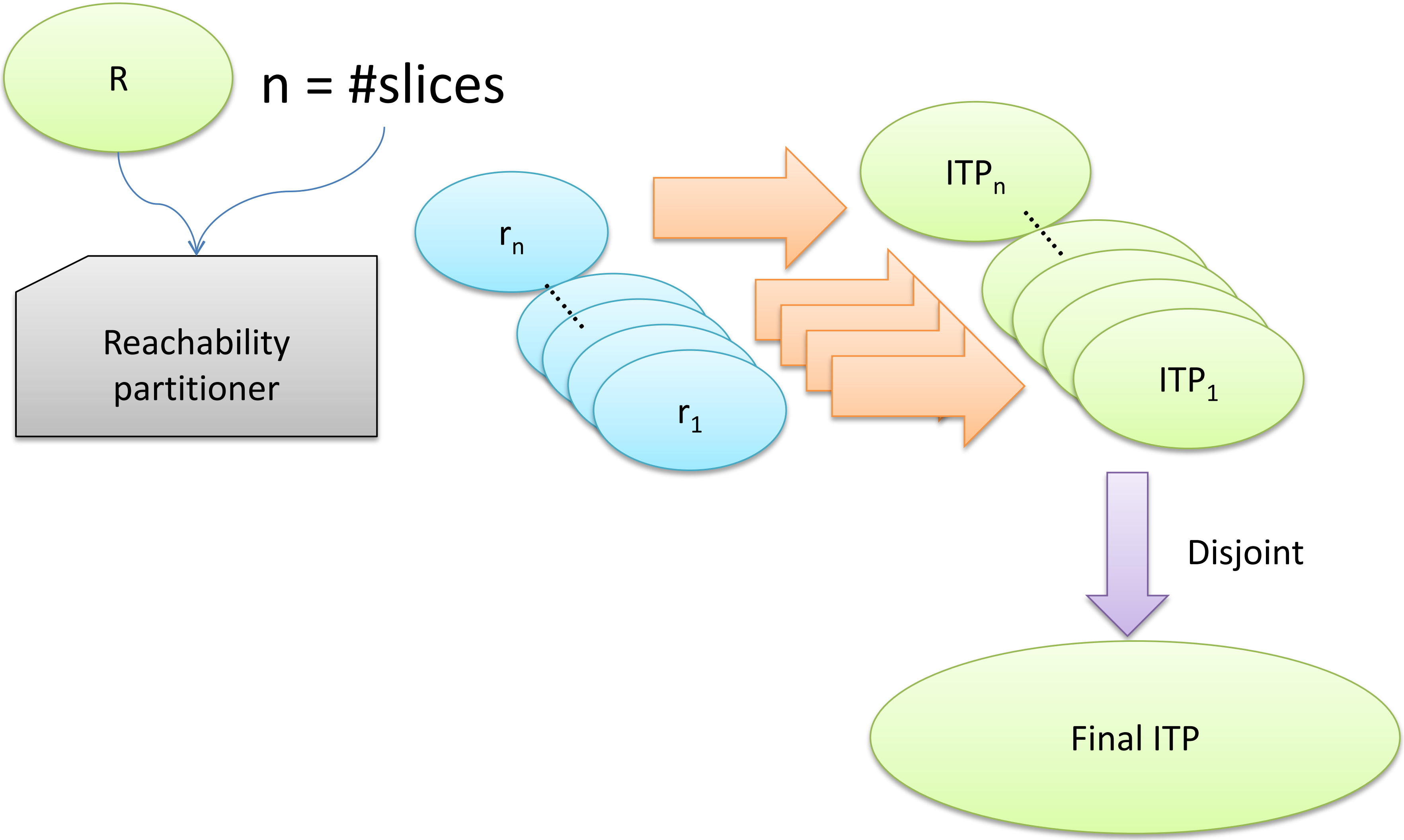


Make Abstraction Coarse

- The disjunction of the reachability becomes coarse than computing R's directly



Flexible Interpolation by Reachability Partitioning



ATR&R INTERPOLATION

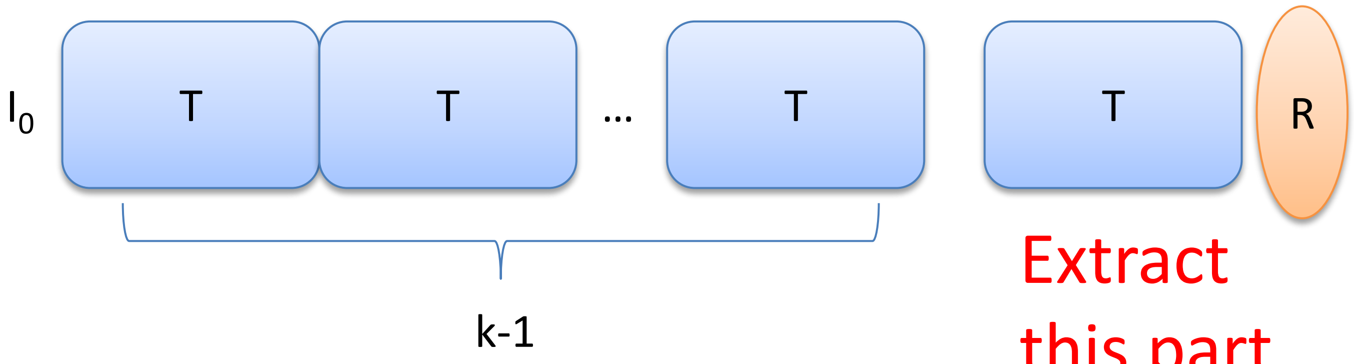
2-Step Interpolation

1. Transition Relation Abstraction

2. Reachability Construction

ATR to ATR Circuit

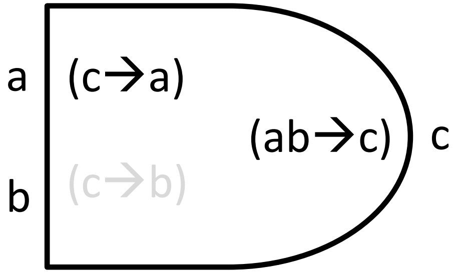
- Extract UNSAT core on the last time-frame



Extract this part

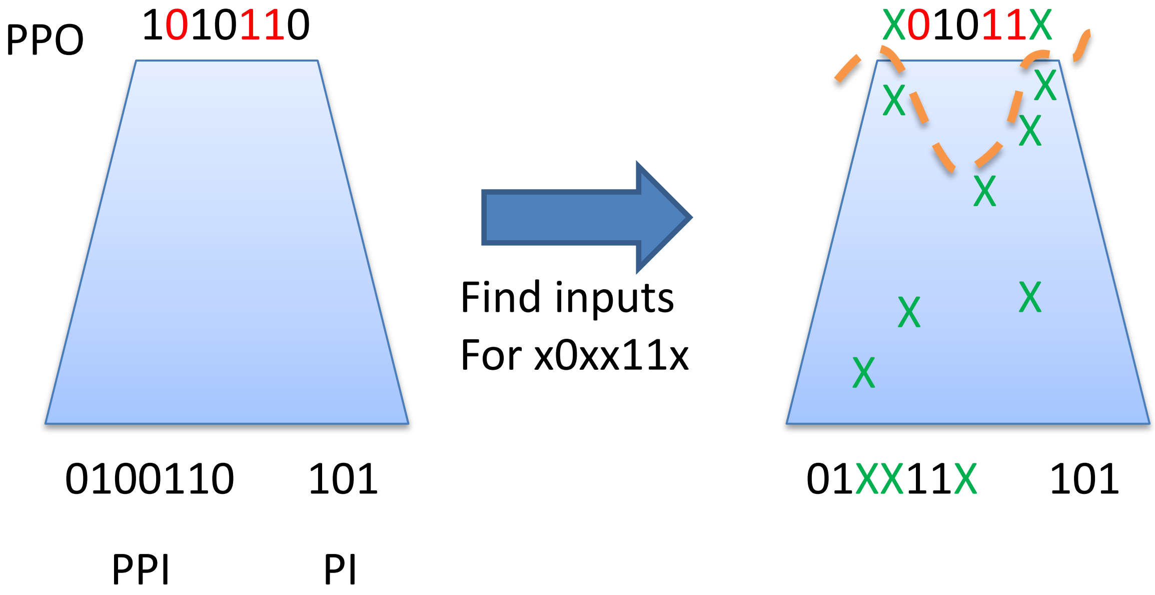
ATR Circuit

- Record the presence of clauses in proof



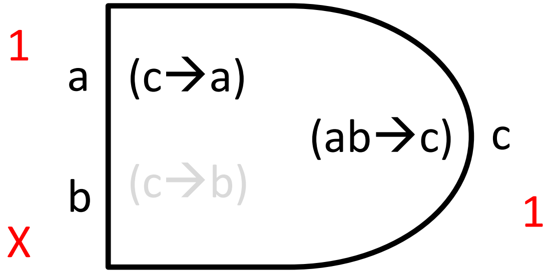
Ternary Simulation

- Finds don't-care state variables



ATR Circuit Simulation

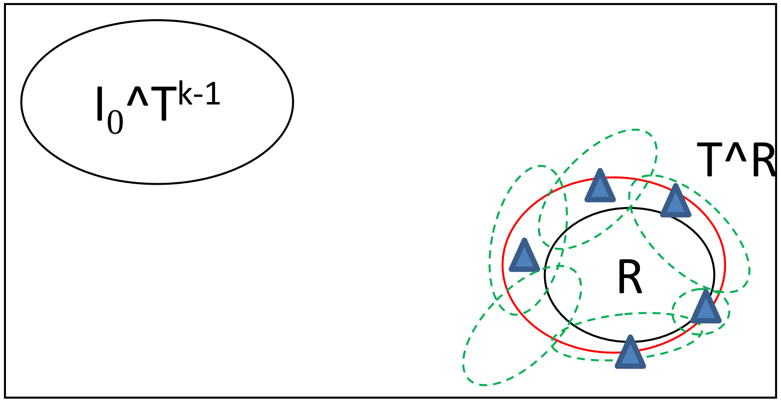
- Similar to ternary simulation
- Consider constrains absent in abstract transition relation



c doesn’t imply b anymore

Interpolant Construction

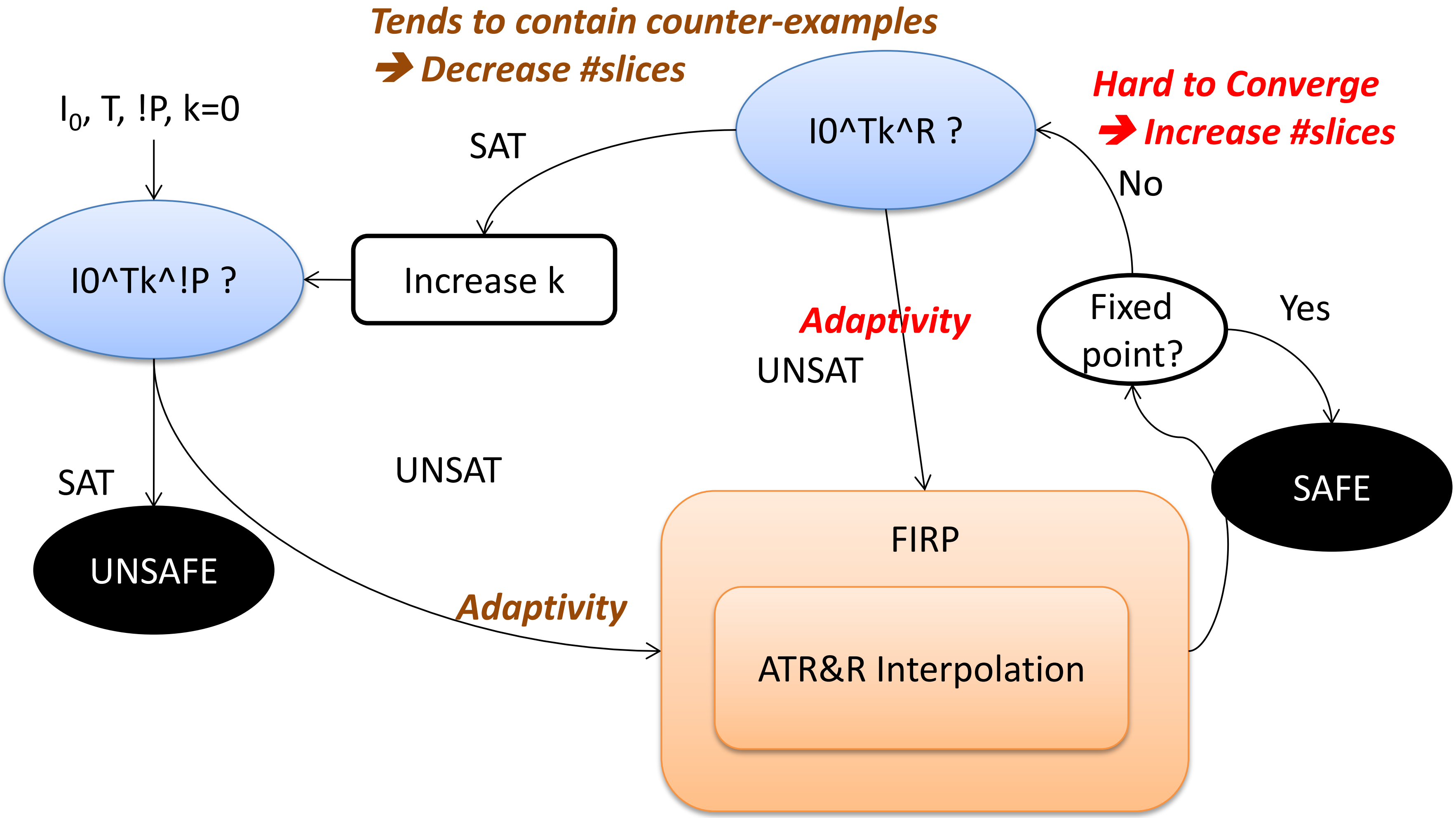
- Iteratively Solve the previous states



After ATR circuit simulation

▲ Minterms

Adaptive IMC Framework (review)



What We Refine

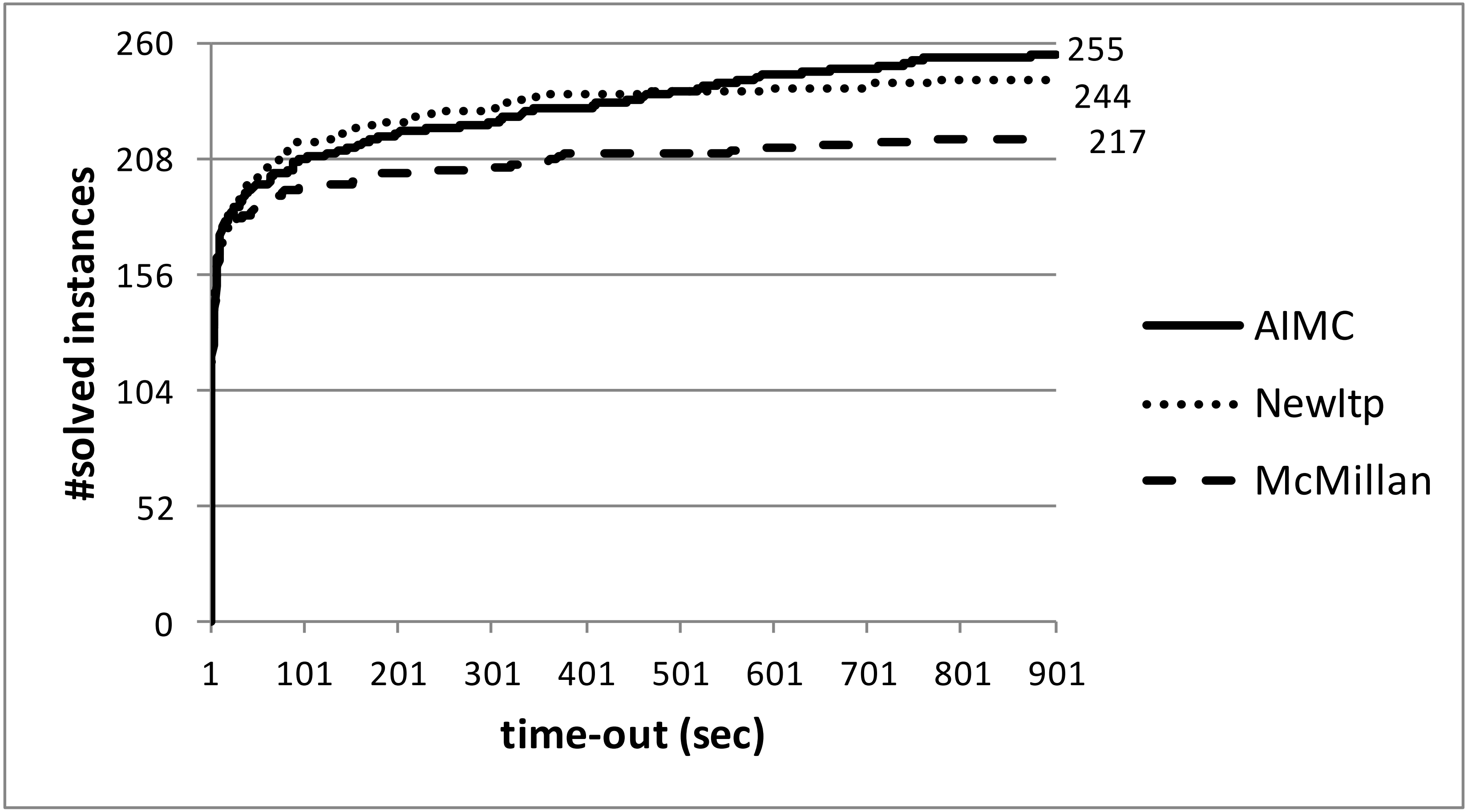
- BMC step
- Interpolation Algorithm

EXPERIMENTAL RESULTS

Experiment Setup

- Intel(R) Xeon(R) CPU E5405, 2.00GHz
- 7GB memory, 15 minutes time-out
- hwmcc11nointel.7z
  - Downloaded from HWMCC website
- Initial number of slice: 1
  - Same as the McMillan's IMC

Comparison in total cases



Statistics in Detail

<table>
<tr><td colspan="4">405 cases in total</td></tr>
<tr><td></td><td>AIMC</td><td>NewITP</td><td>McMillan</td></tr>
<tr><td>All Solved</td><td colspan="3">179</td></tr>
<tr><td>Solved only</td><td>20</td><td>14</td><td>7</td></tr>
<tr><td>Unsolved only</td><td>13</td><td>18</td><td>38</td></tr>
<tr><td>All Unsolved</td><td colspan="3">116</td></tr>
<tr><td colspan="4">100 cases unsolved by PDR</td></tr>
<tr><td></td><td>AIMC</td><td>NewITP</td><td>McMillan</td></tr>
<tr><td>Solved</td><td>15</td><td>7</td><td>12</td></tr>
</table>

CONCLUSION

Contribution

- Adaptive interpolation framework
- Abstraction degree manipulation
- Enhancement of IMC
  - Solve the most instances in total
  - Solve the most instances hard for PDR

Novelty

- Flexible interpolation by reachability partitioning

- 2-phase interpolation

- 1-way SAT/UNSAT generalization by only one-time simulation

Thanks for Your Attention!