

Combining CEGAR and Lazy Abstraction for Verifying Timed Systems

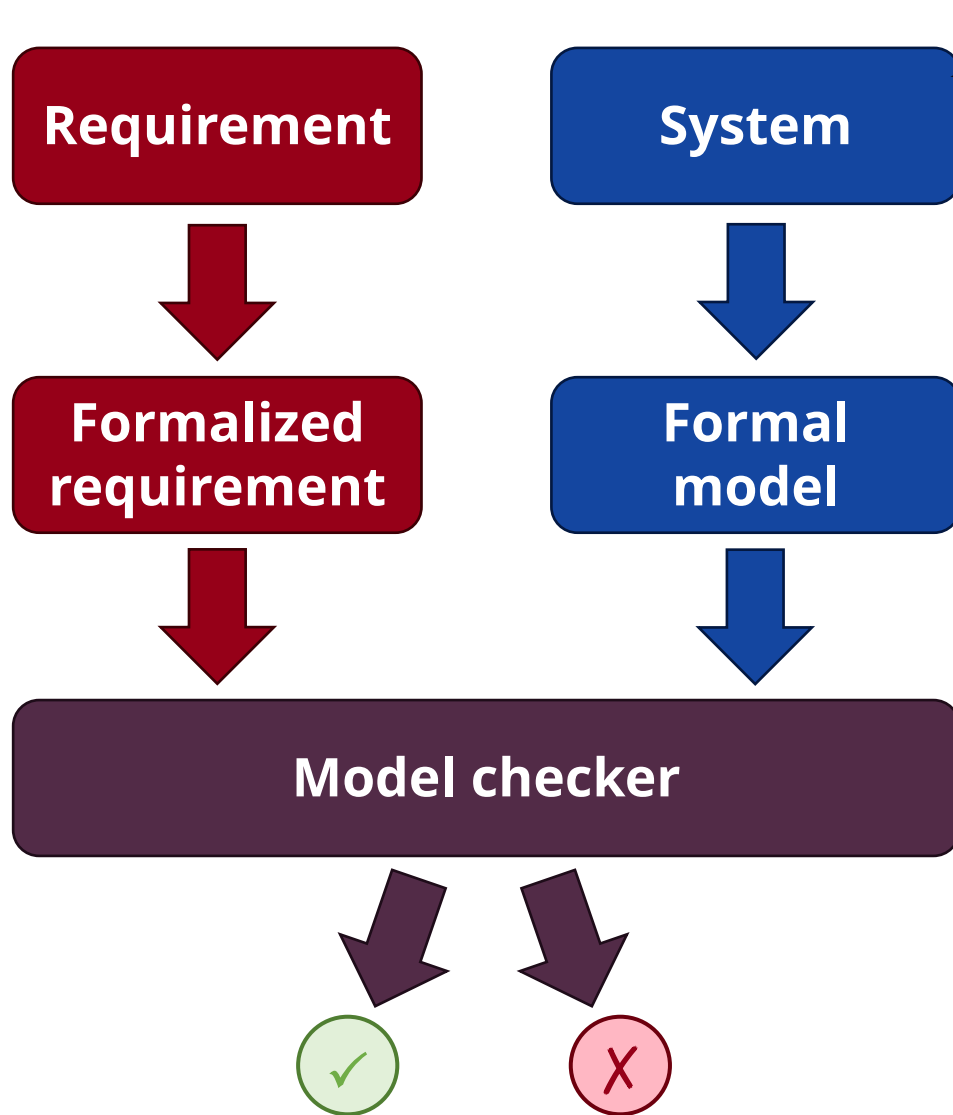
Dóra Cziborová



Budapest University of Technology and Economics
Department of Measurement and Information Systems
Critical Systems Research Group



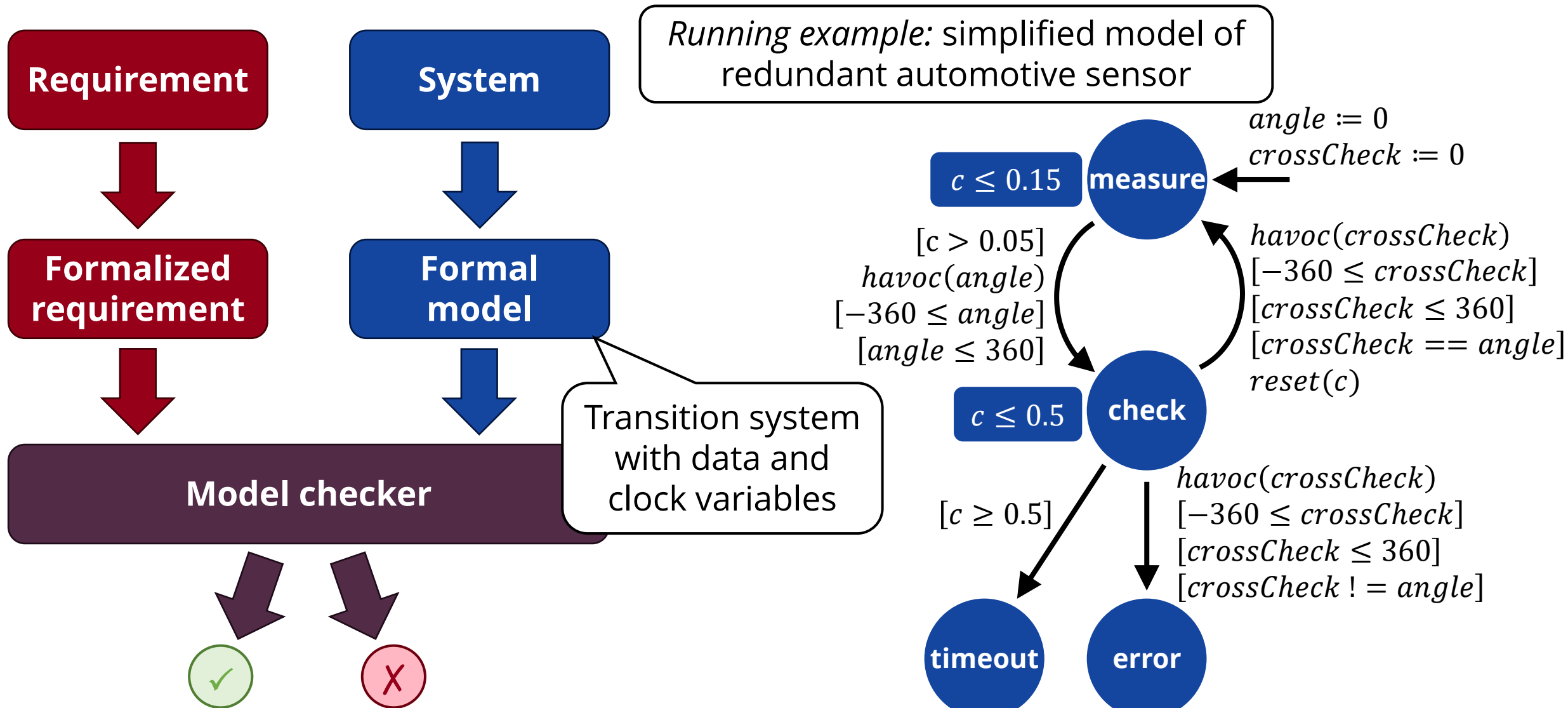
Verification of Timed Systems by Model Checking



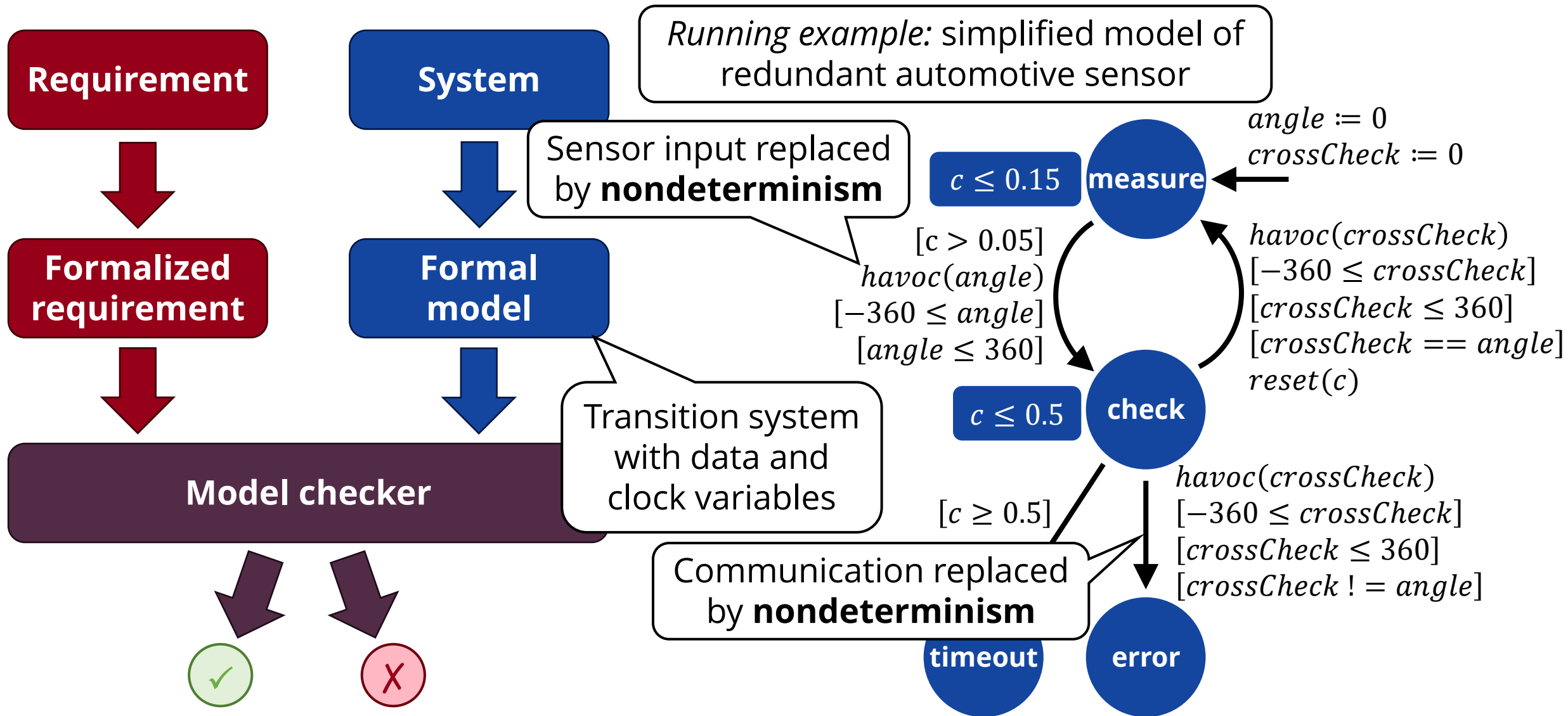
Real-time software-intensive systems

- Complex timed behaviors and computations with external data (sensor inputs)
- System models specified by higher-level formalisms, e.g.,
 - **XTA** composite models
 - Block diagrams and **timed statecharts** from **systems engineering** tools
- *Examples:* railway communication protocols, safety-critical automotive subsystems

Verification of Timed Systems by Model Checking



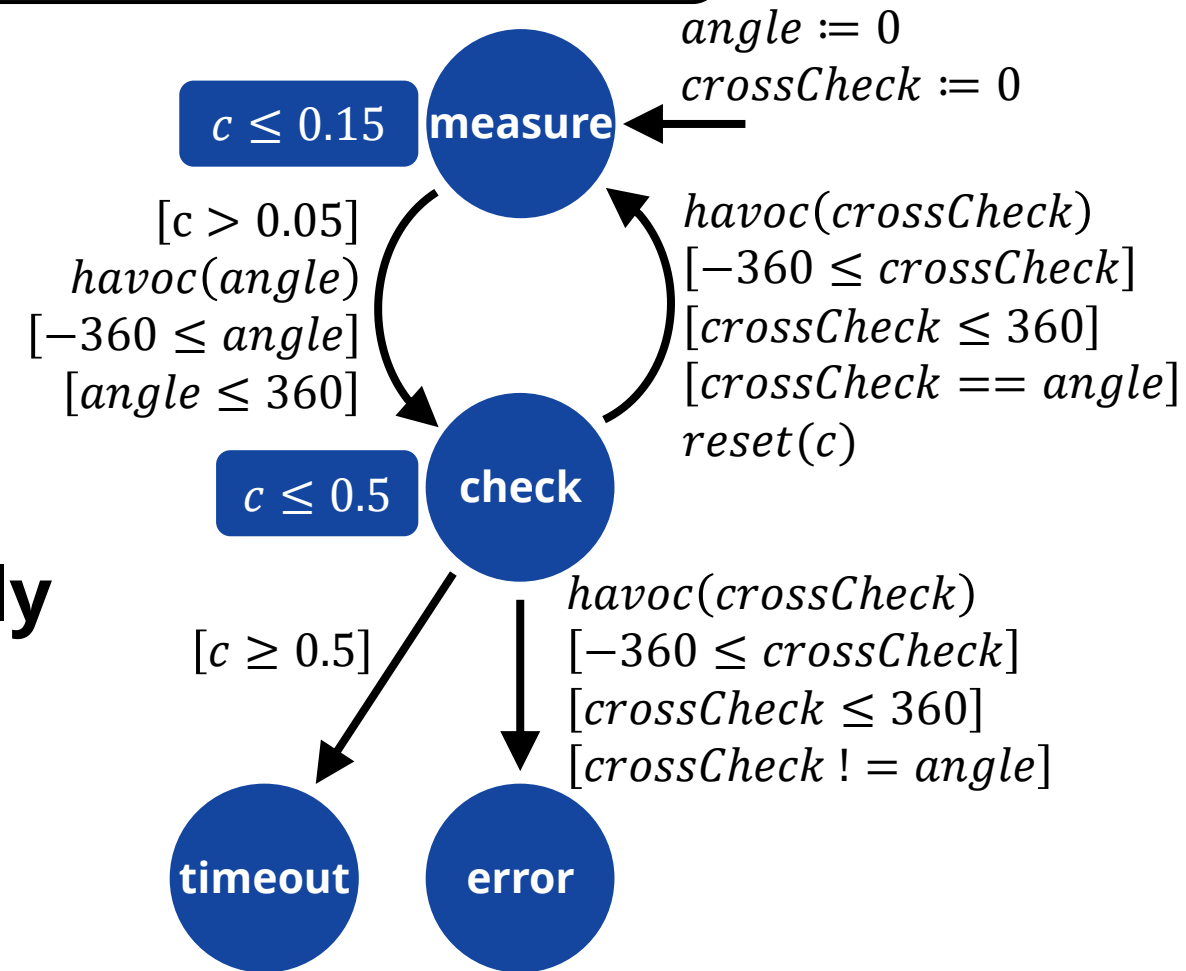
Verification of Timed Systems by Model Checking



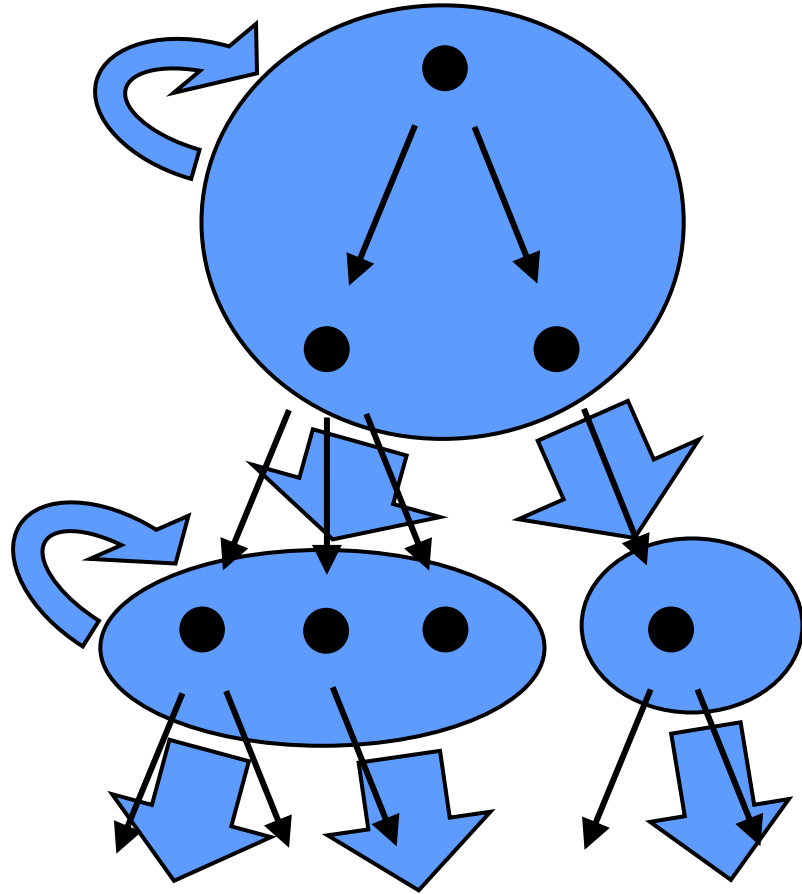
Challenges of Verifying Timed Systems

Running example: simplified model of redundant automotive sensor

- 1) Data variables:
 - **State space explosion**
- 2) Clock variables:
 - **Continuous** variables
 - Reasoning with an **uncountably infinite set of states**



Abstraction, Abstract Reachability Graph



Abstraction-based methods:

- An **abstract state** may represent multiple concrete states
- State space exploration: **abstract reachability graph (ARG)** of abstract states and transitions

Abstract Domains

Explicit value abstraction

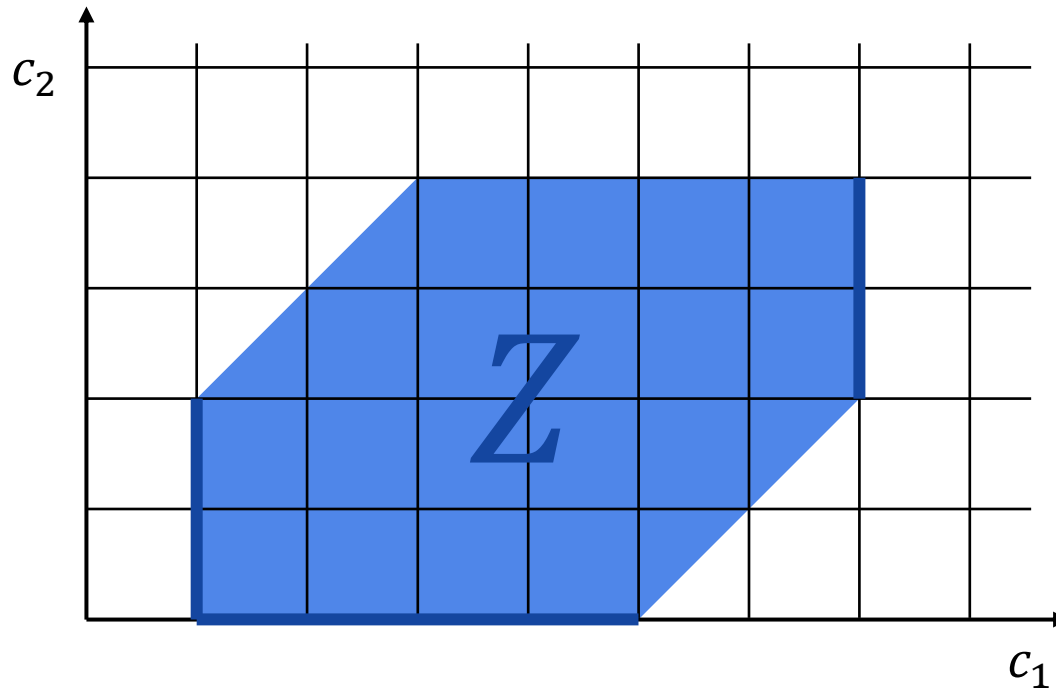
Predicate abstraction

Zone abstraction

Abstract Domain for Time Abstraction

Zone abstraction

A set of clock valuations

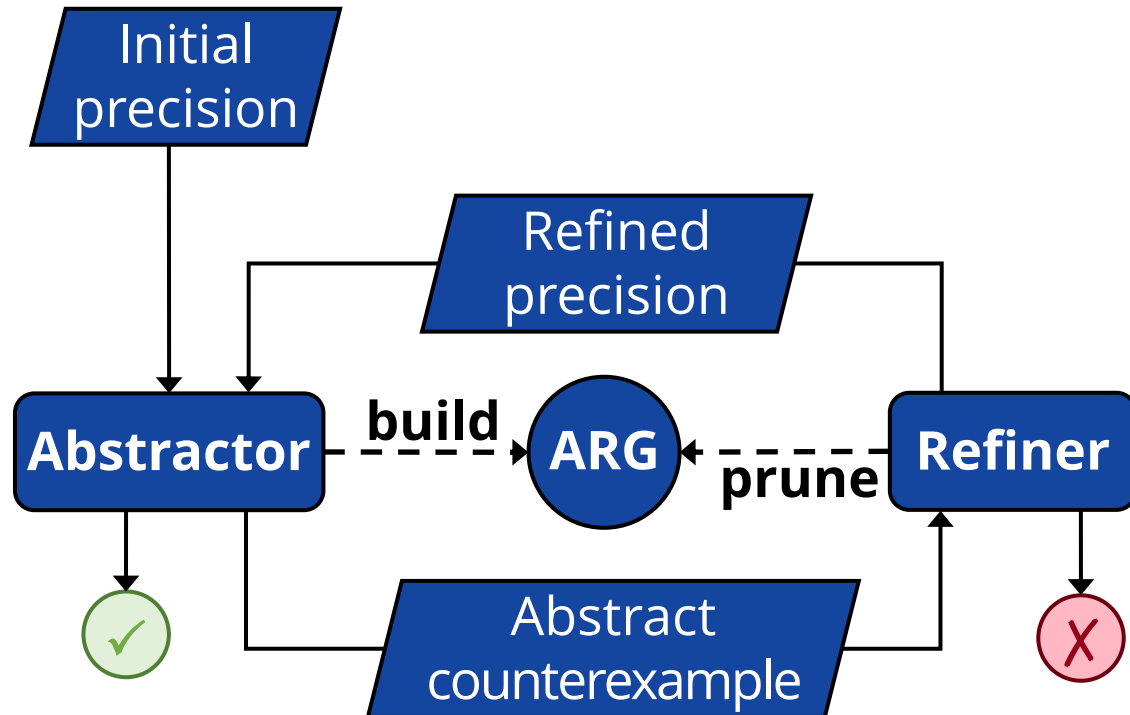


The same set of clock valuations
as a set of clock constraints

$$\left. \begin{array}{l} c_1 \leq 7 \\ c_1 \geq 1 \\ c_2 < 4 \\ c_2 \geq 0 \\ c_2 - c_1 < 1 \\ c_1 - c_2 < 5 \end{array} \right\} Z$$

CEGAR

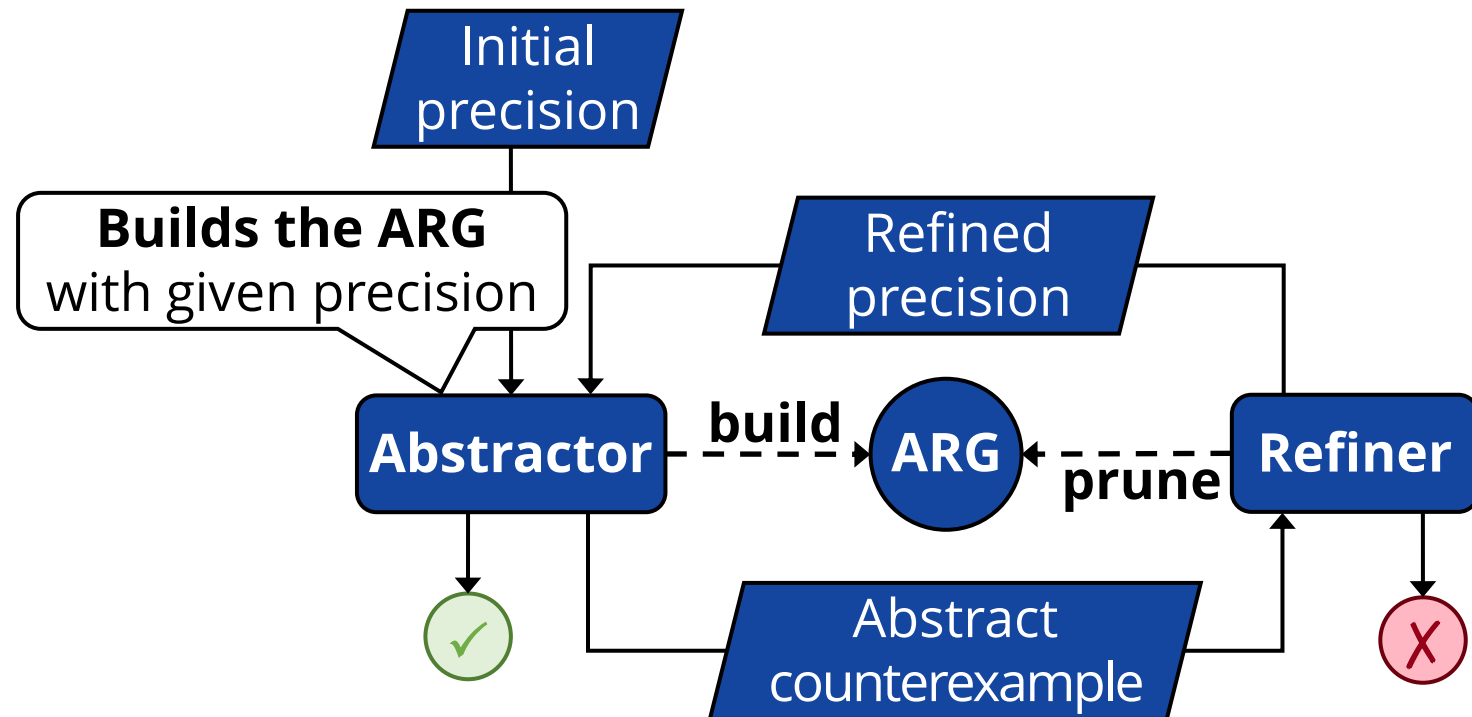
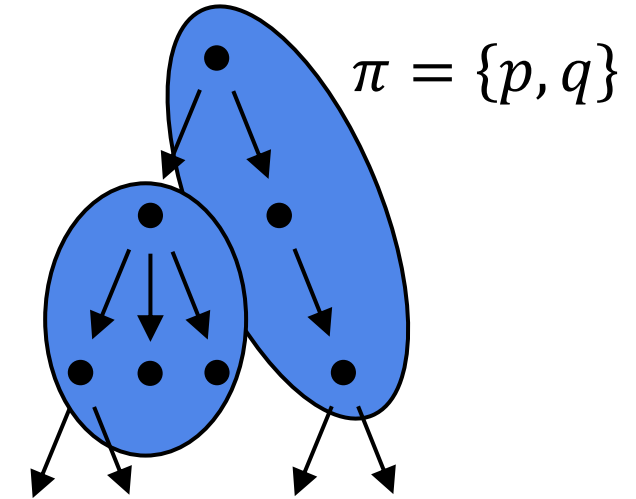
(CounterExample-Guided Abstraction Refinement)



CEGAR

(CounterExample-Guided Abstraction Refinement)

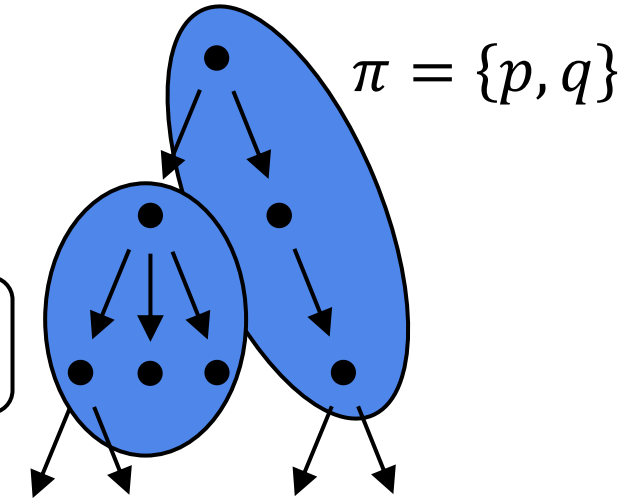
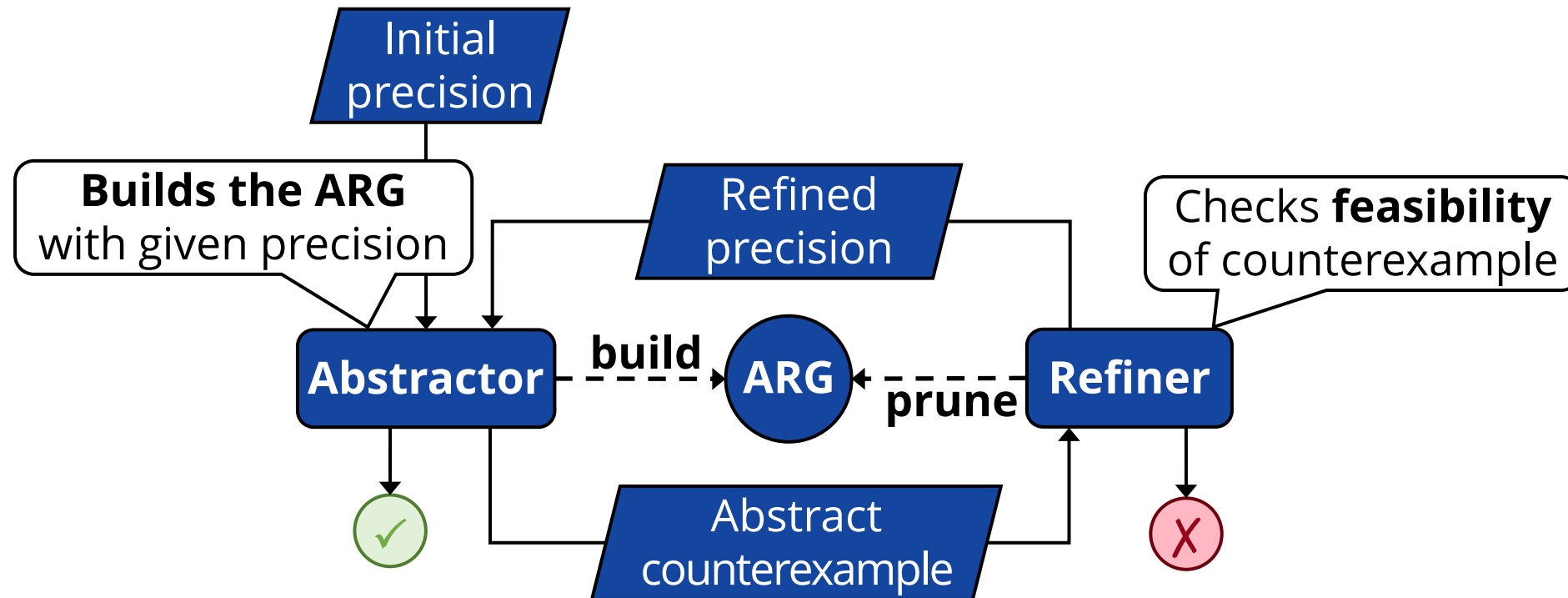
Precision
e.g. a set of predicates



CEGAR

(CounterExample-Guided Abstraction Refinement)

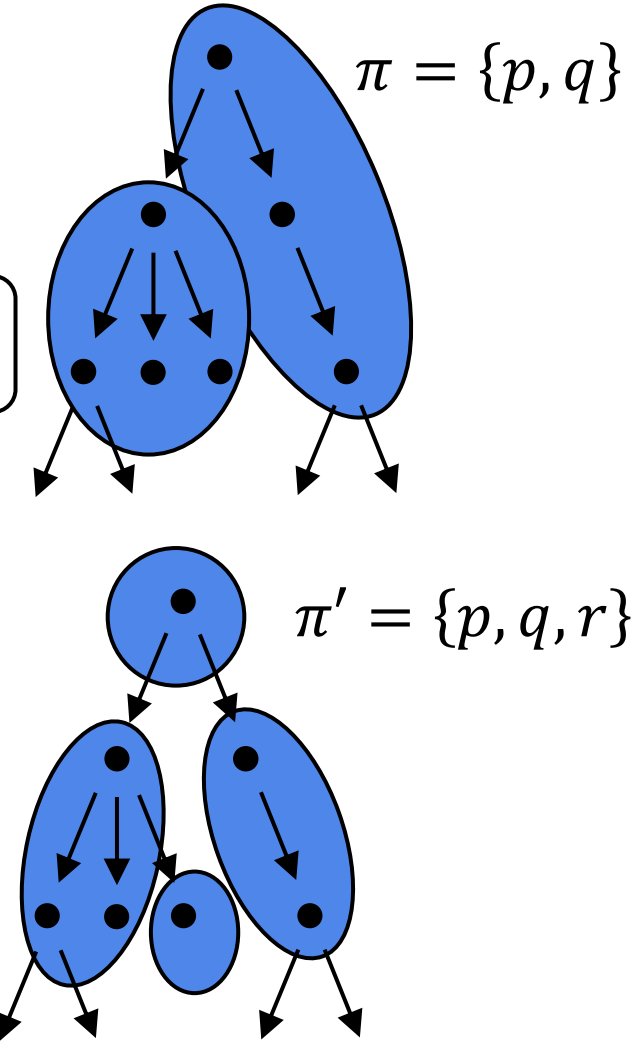
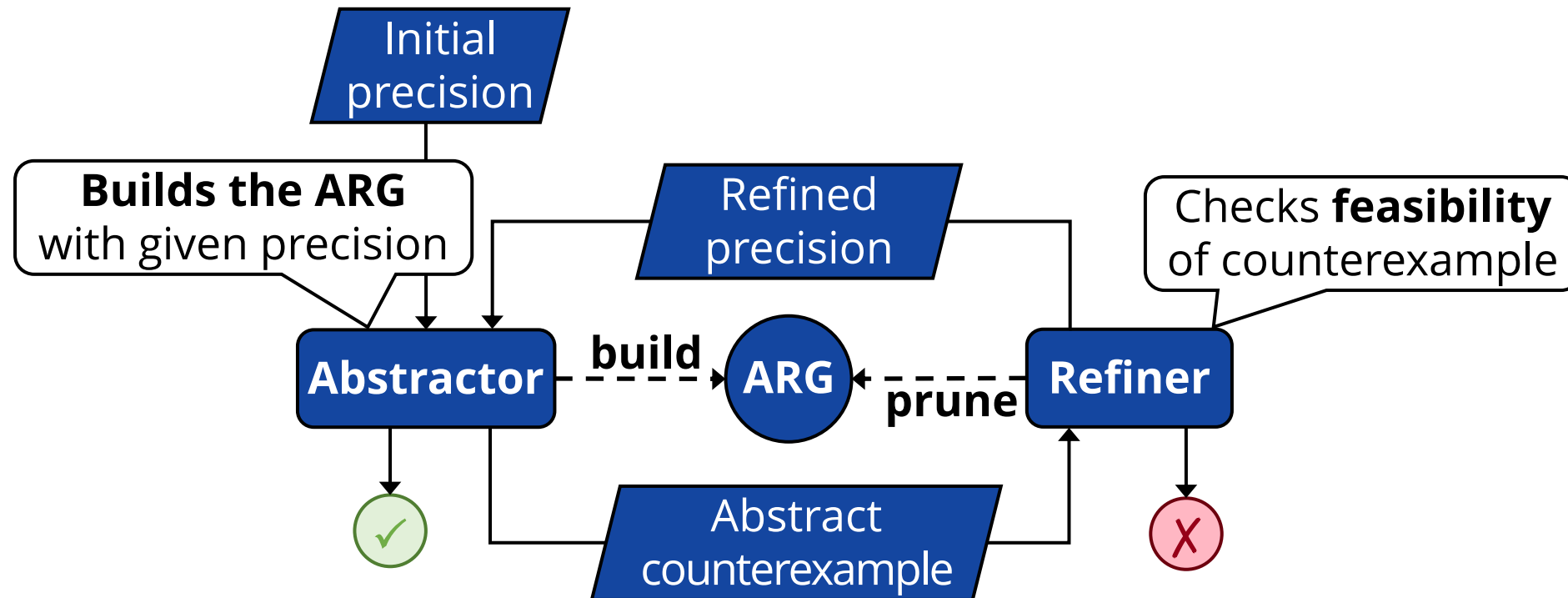
Precision
e.g. a set of predicates



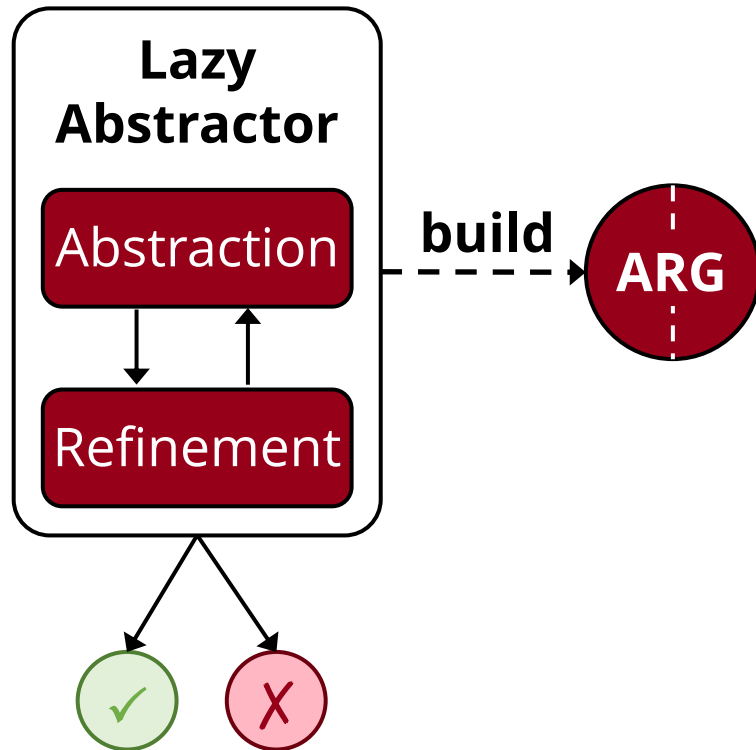
CEGAR

(CounterExample-Guided Abstraction Refinement)

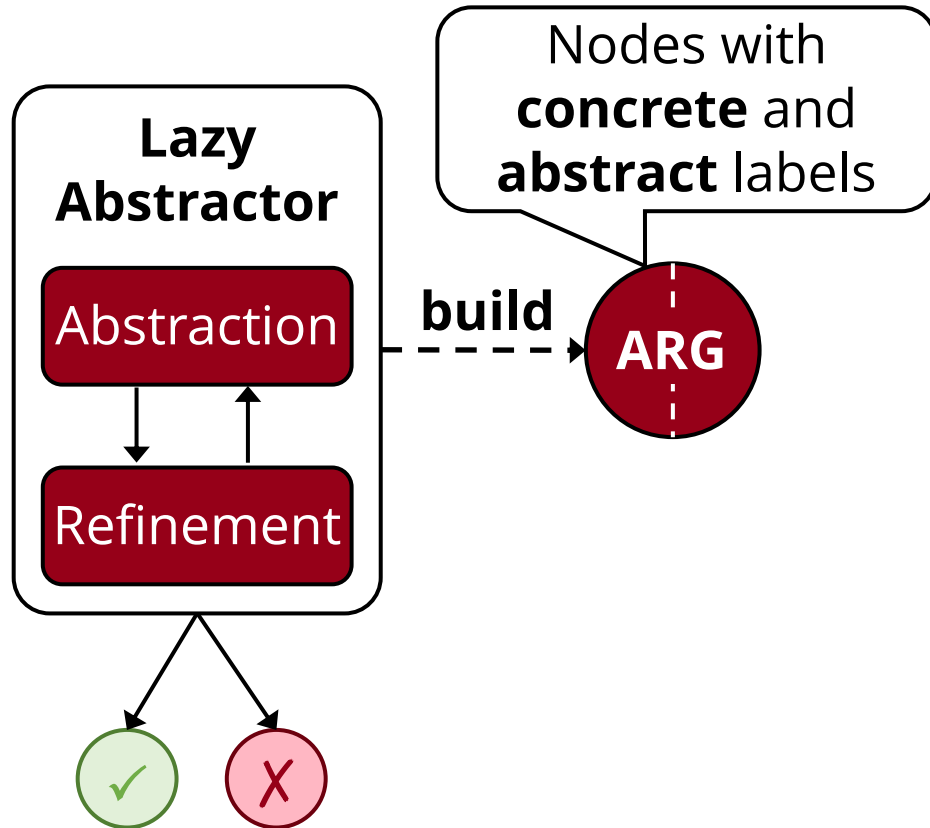
Precision
e.g. a set of predicates



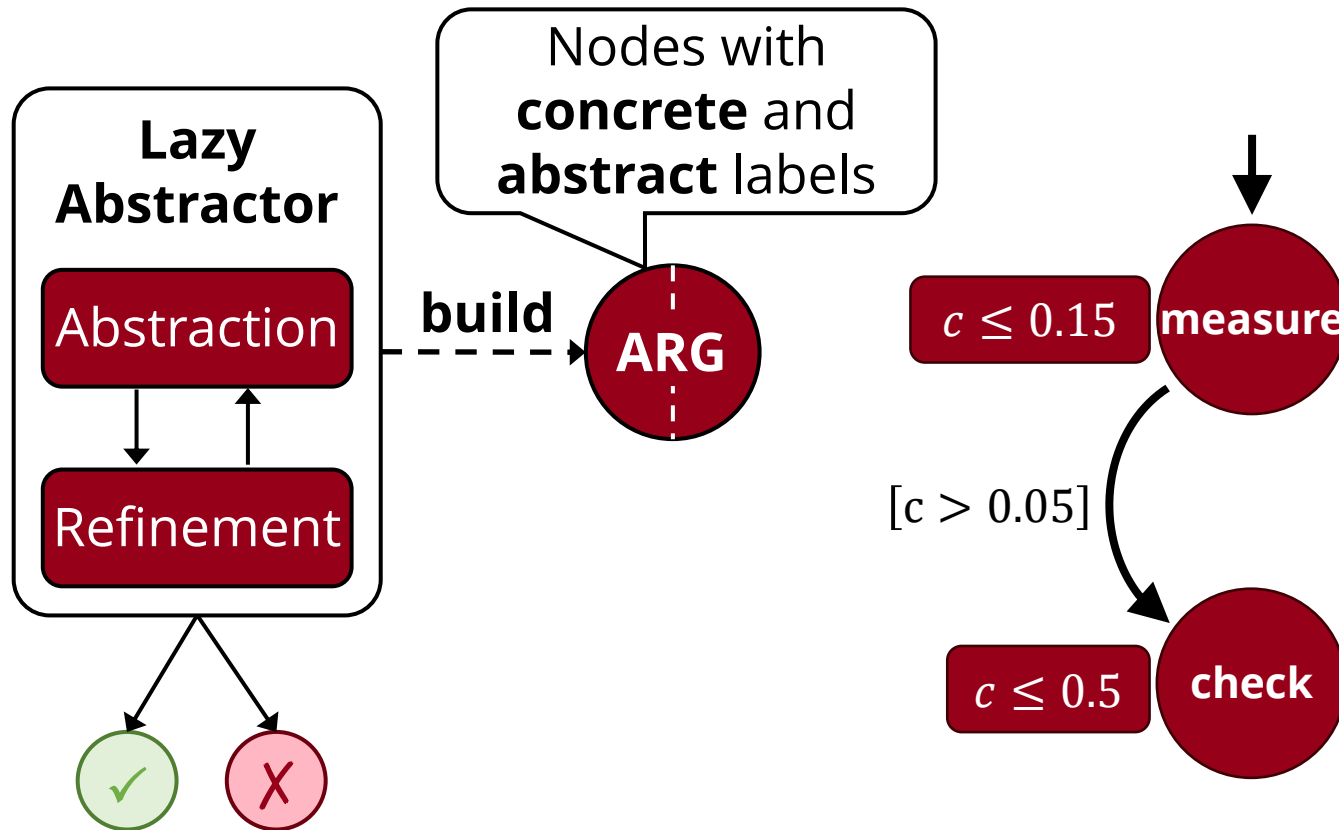
Lazy Abstraction



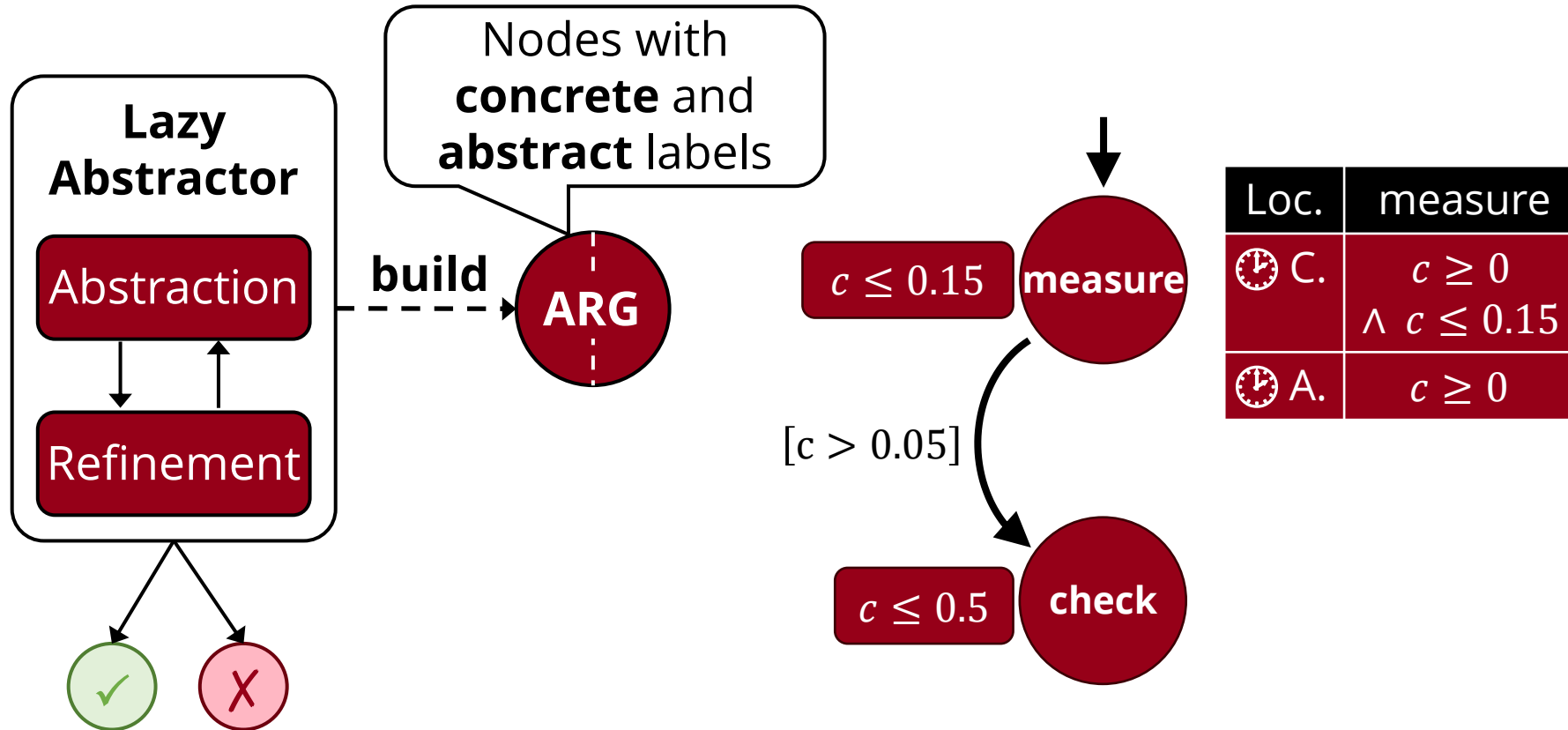
Lazy Abstraction



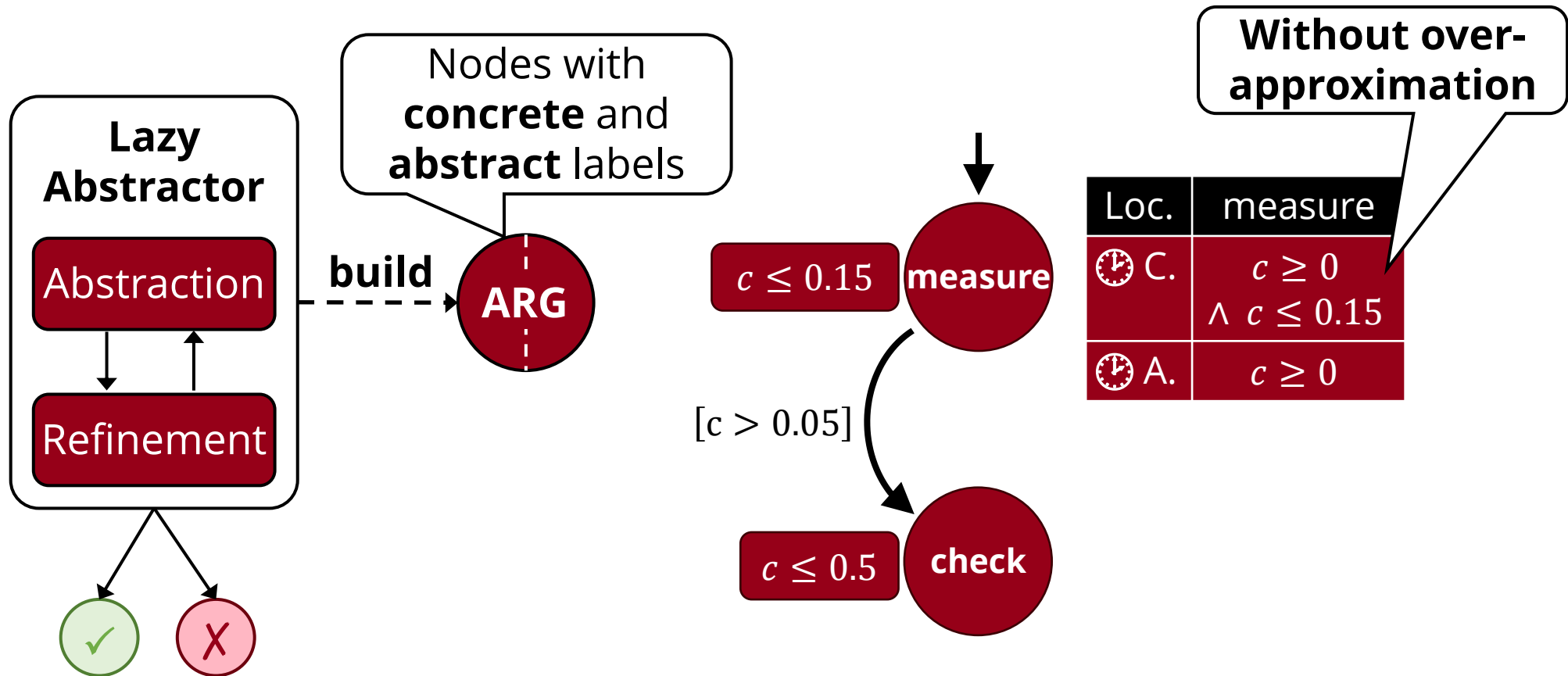
Lazy Abstraction



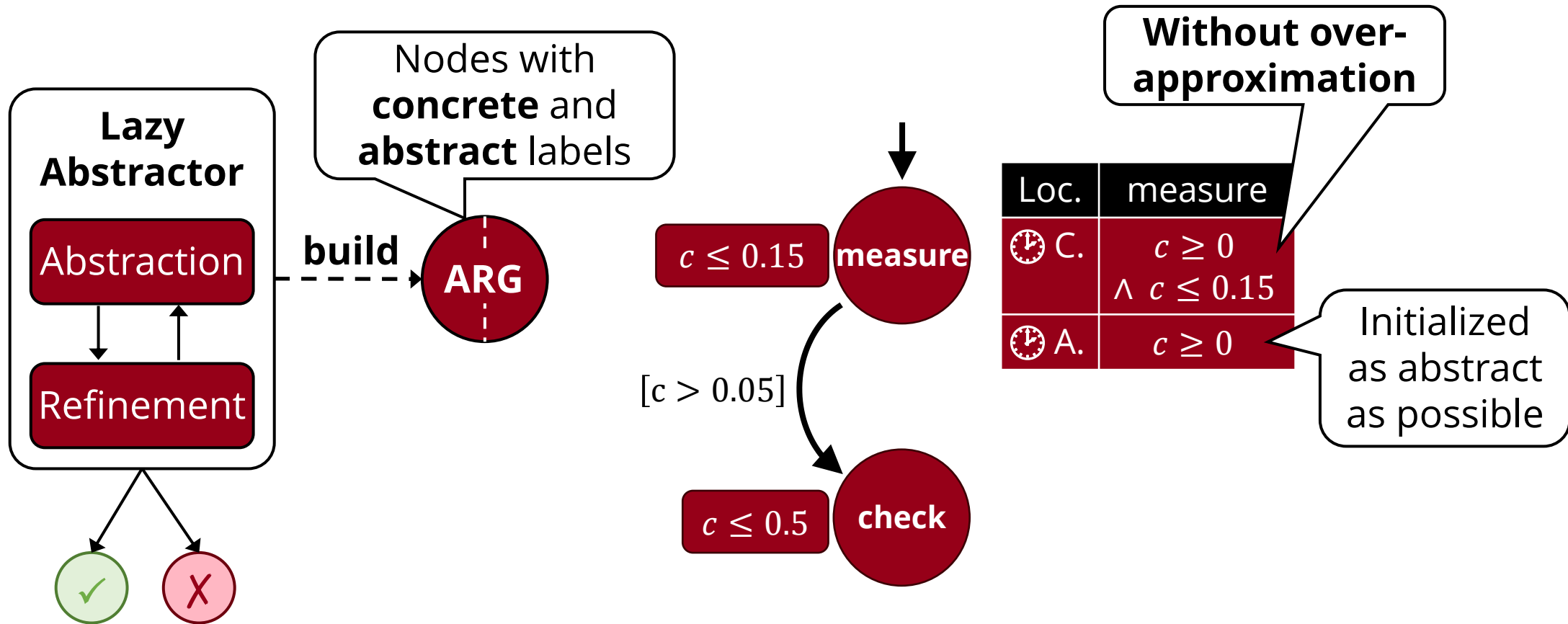
Lazy Abstraction



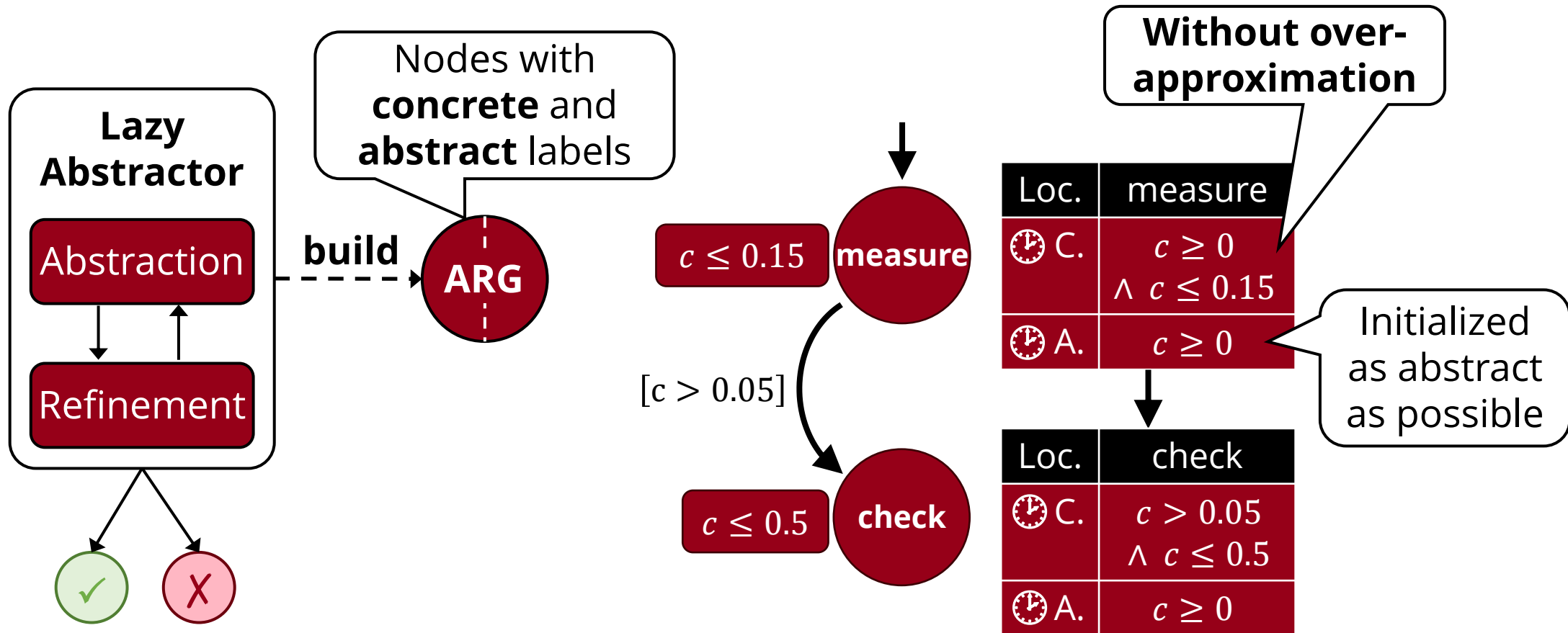
Lazy Abstraction



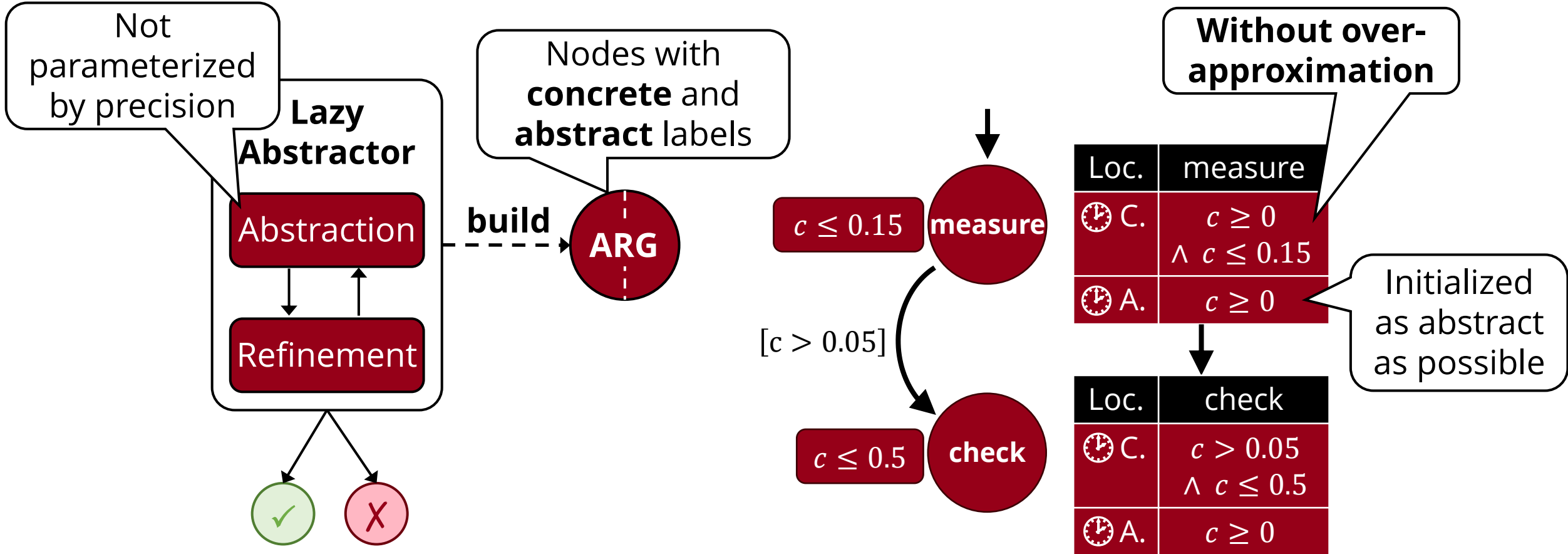
Lazy Abstraction



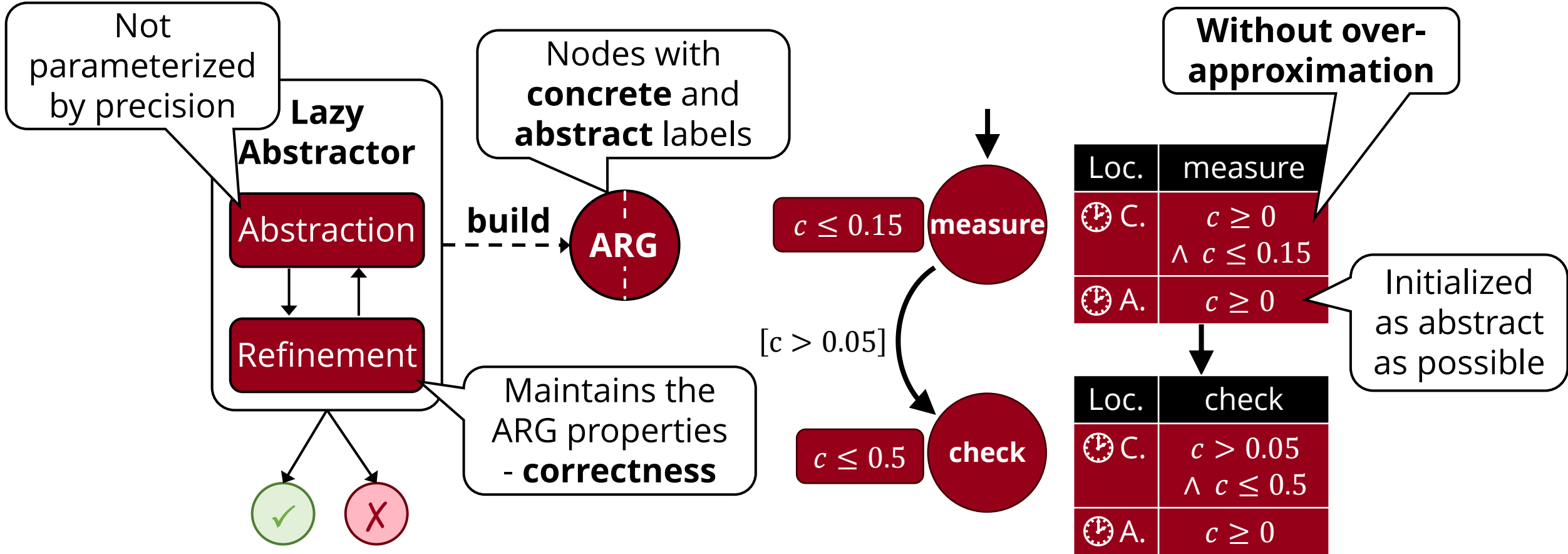
Lazy Abstraction



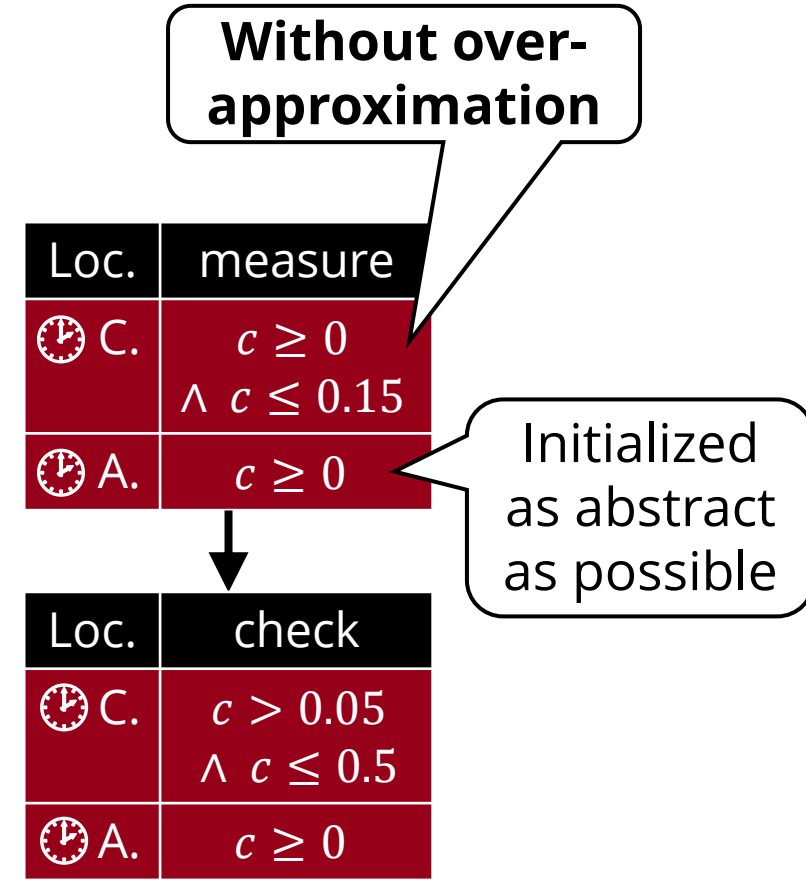
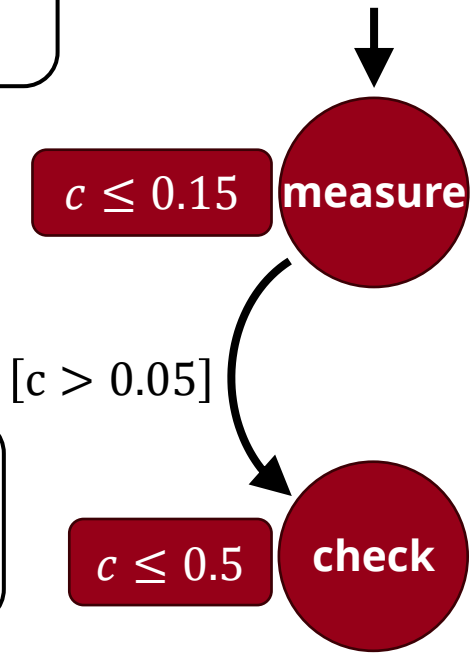
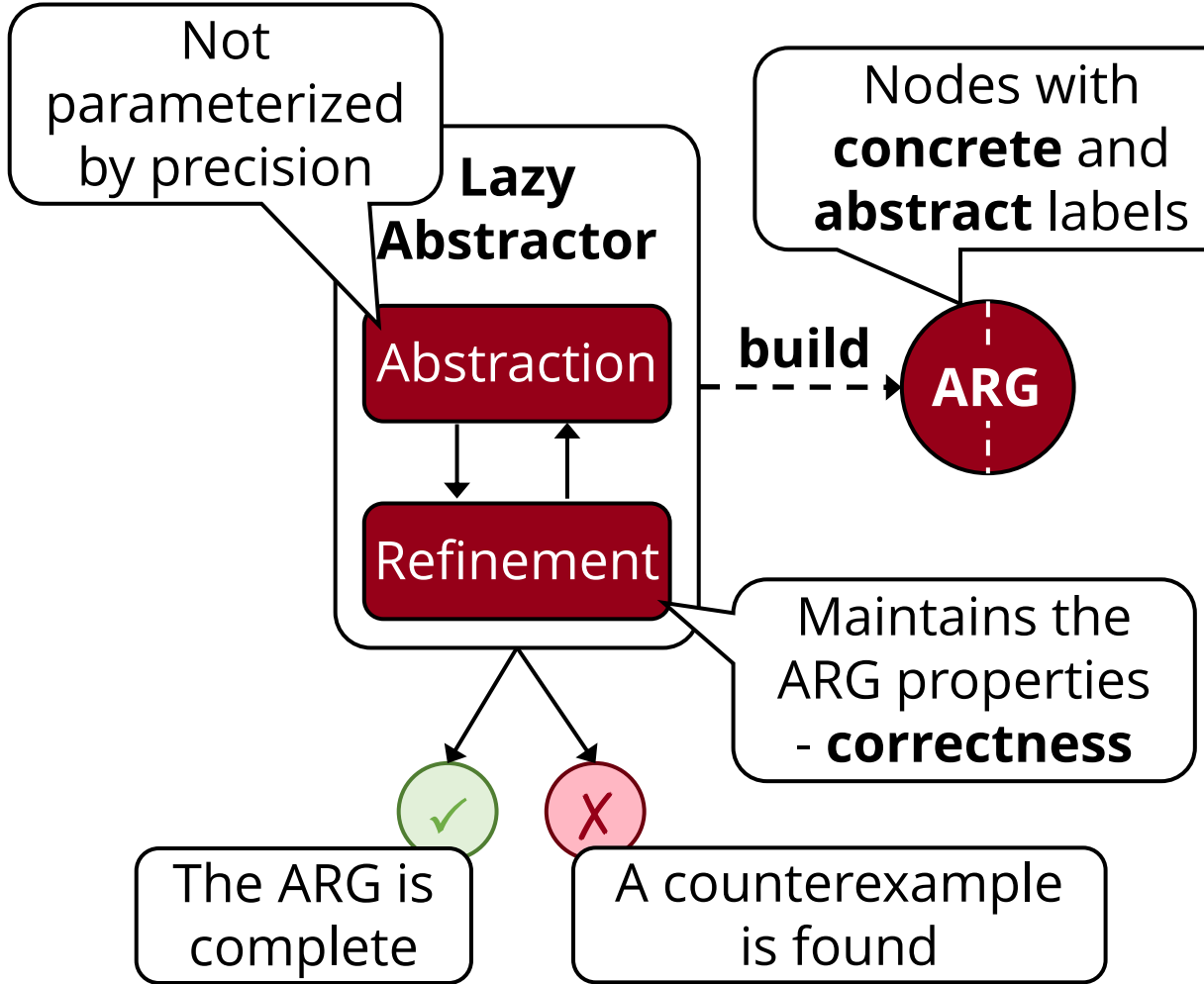
Lazy Abstraction



Lazy Abstraction



Lazy Abstraction



CEGAR

Lazy abstraction

Time abstraction

Requires defining precision
→ **inefficient refinement**
techniques



Efficient abstraction and
refinement techniques



Data abstraction

Efficient, supports
a wide set of
expressive abstractions



Either **inefficient refinement**
techniques, or has
limited expressiveness



CEGAR

Lazy abstraction

Time abstraction

Requires defining precision
→ **inefficient refinement**
techniques



Efficient abstraction and
refinement techniques



Data abstraction

Efficient, supports
a wide set of
expressive abstractions

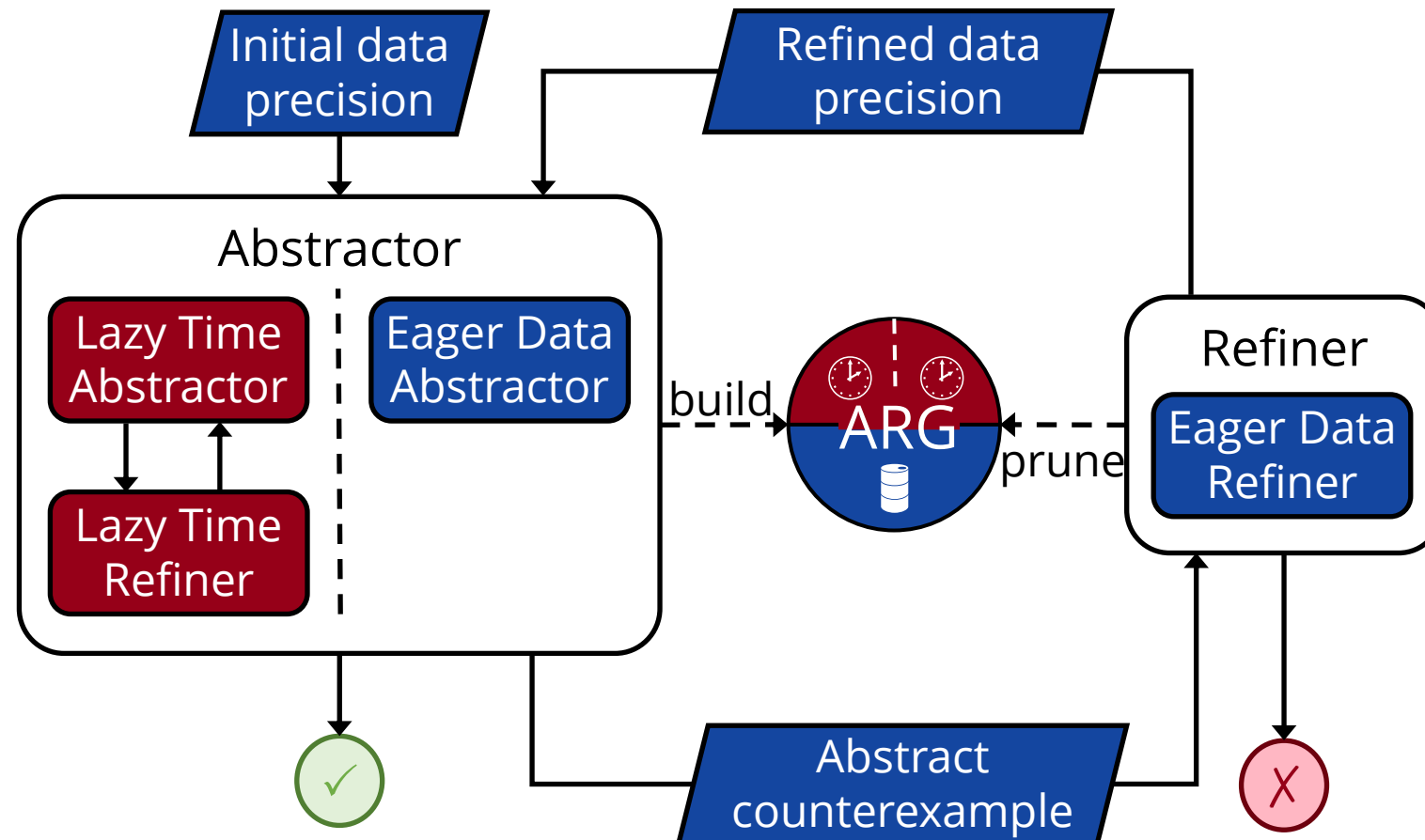


Either **inefficient refinement**
techniques, or has
limited expressiveness



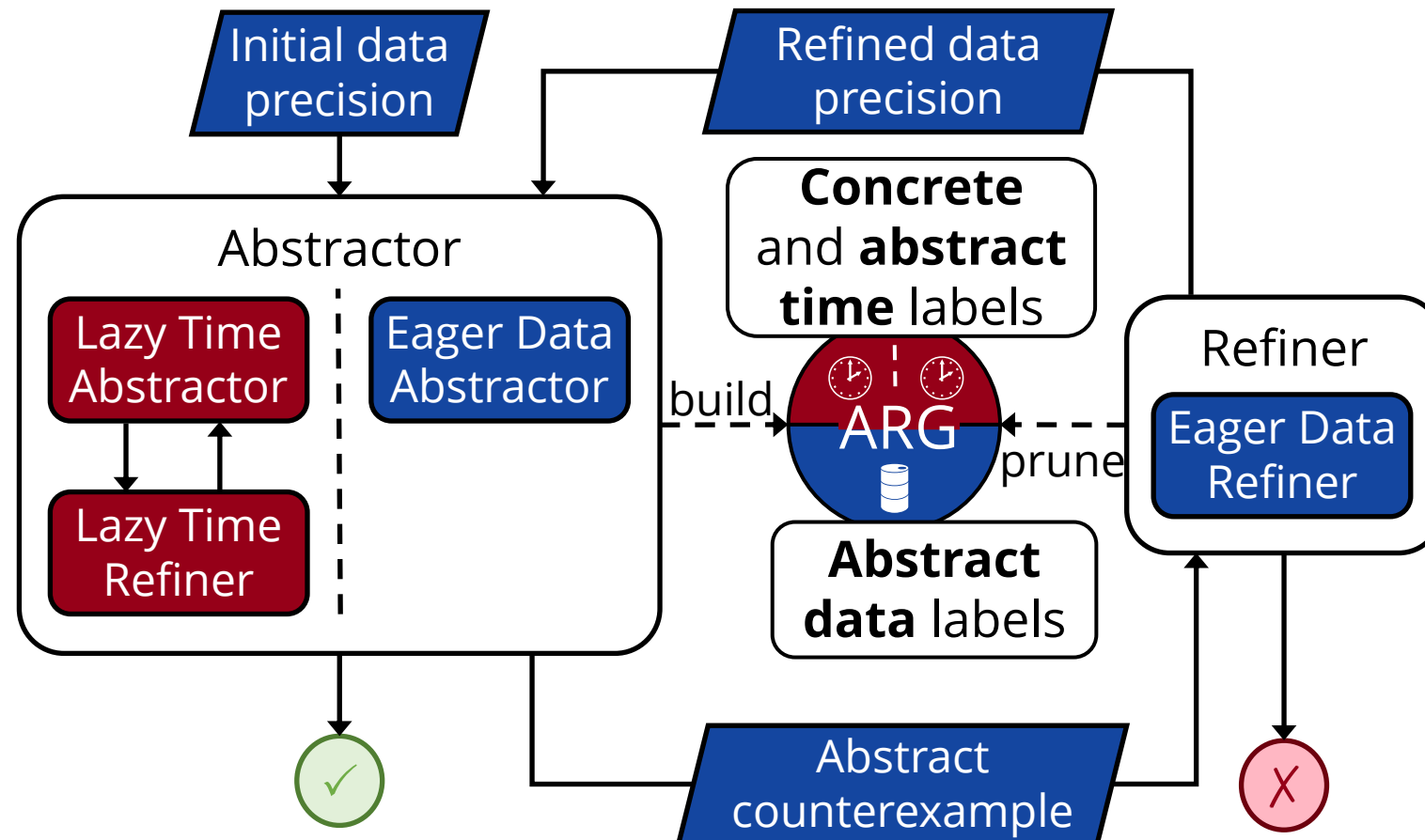
Combining CEGAR and Lazy Abstraction

CEGAR on **data** projection, **lazy abstraction** on **time** projection



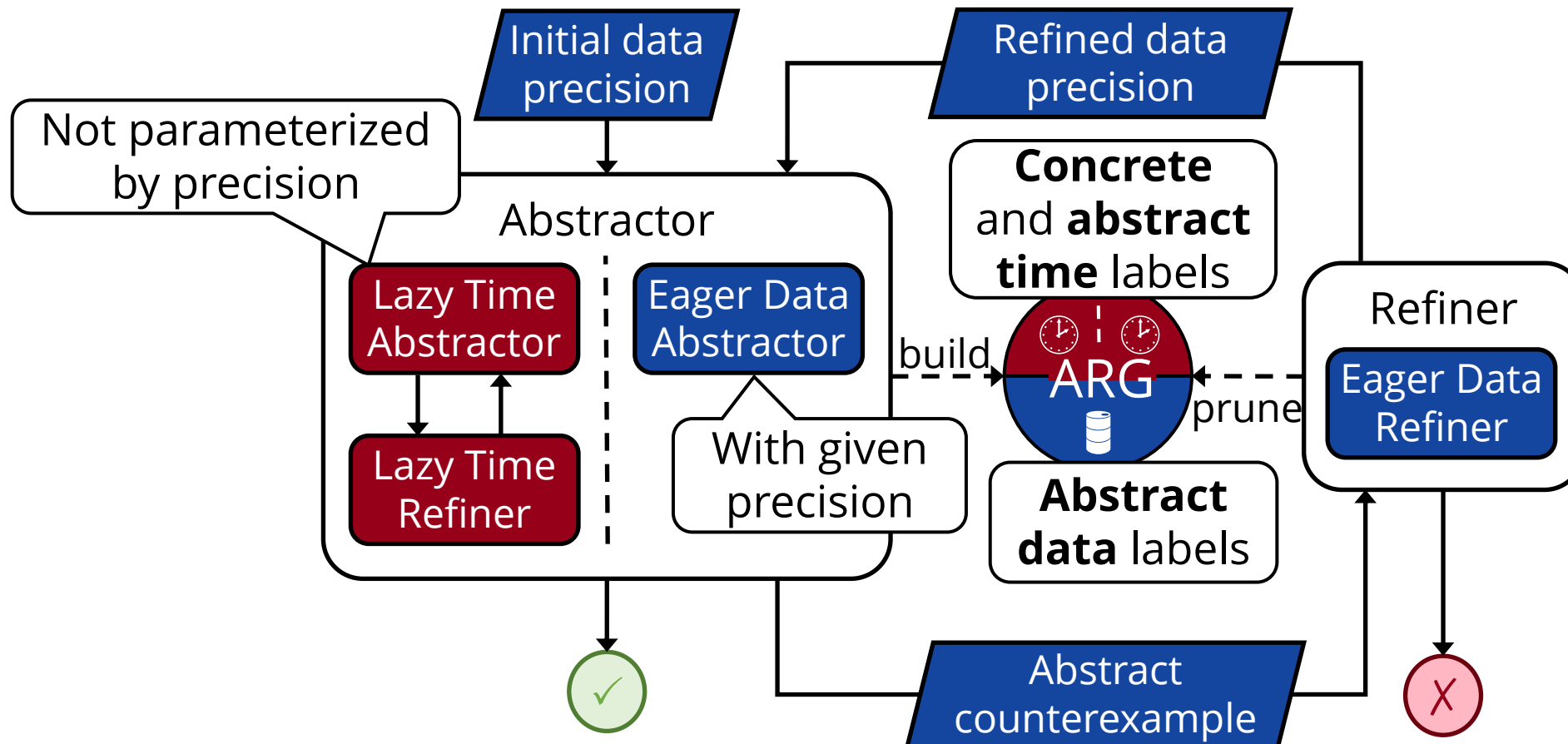
Combining CEGAR and Lazy Abstraction

CEGAR on **data** projection, **lazy abstraction** on **time** projection



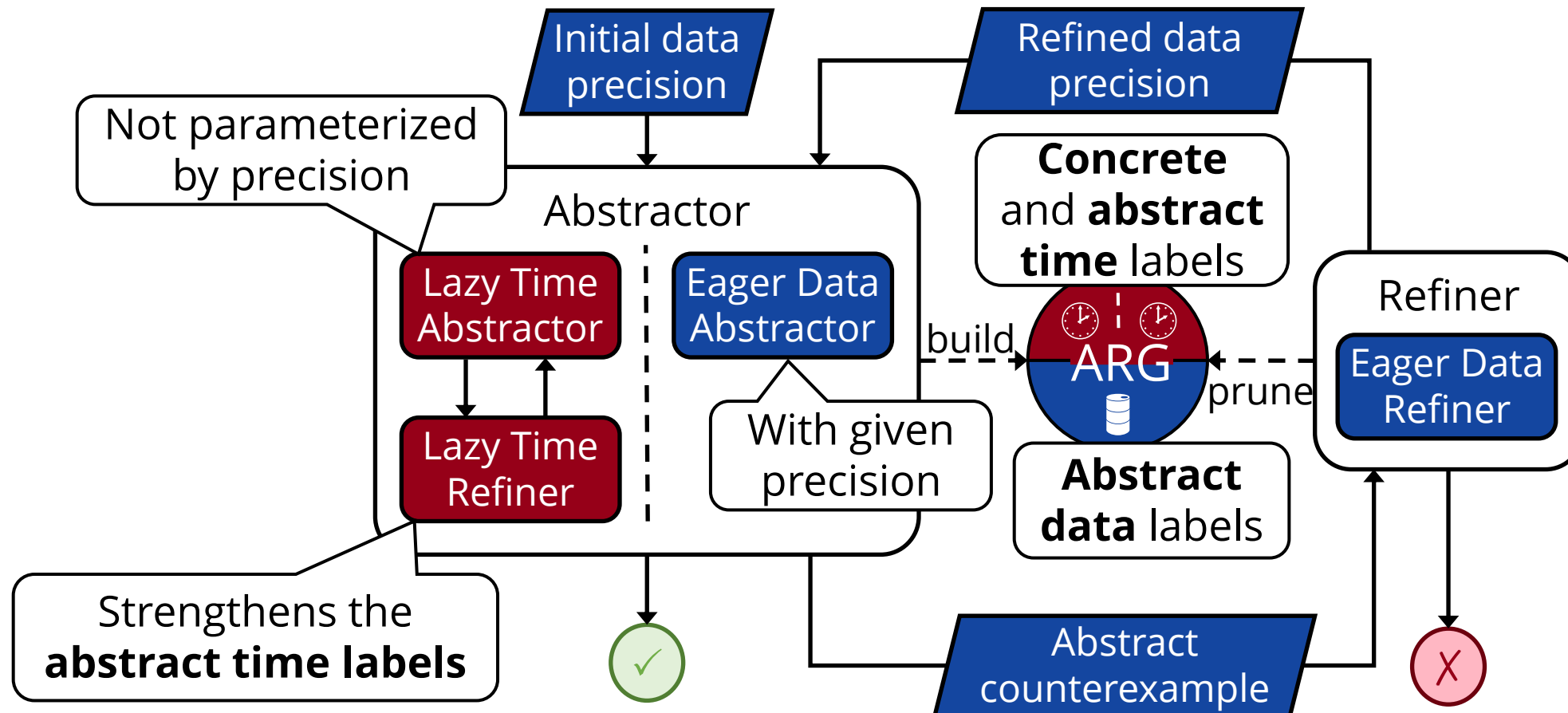
Combining CEGAR and Lazy Abstraction

CEGAR on **data** projection, **lazy abstraction** on **time** projection



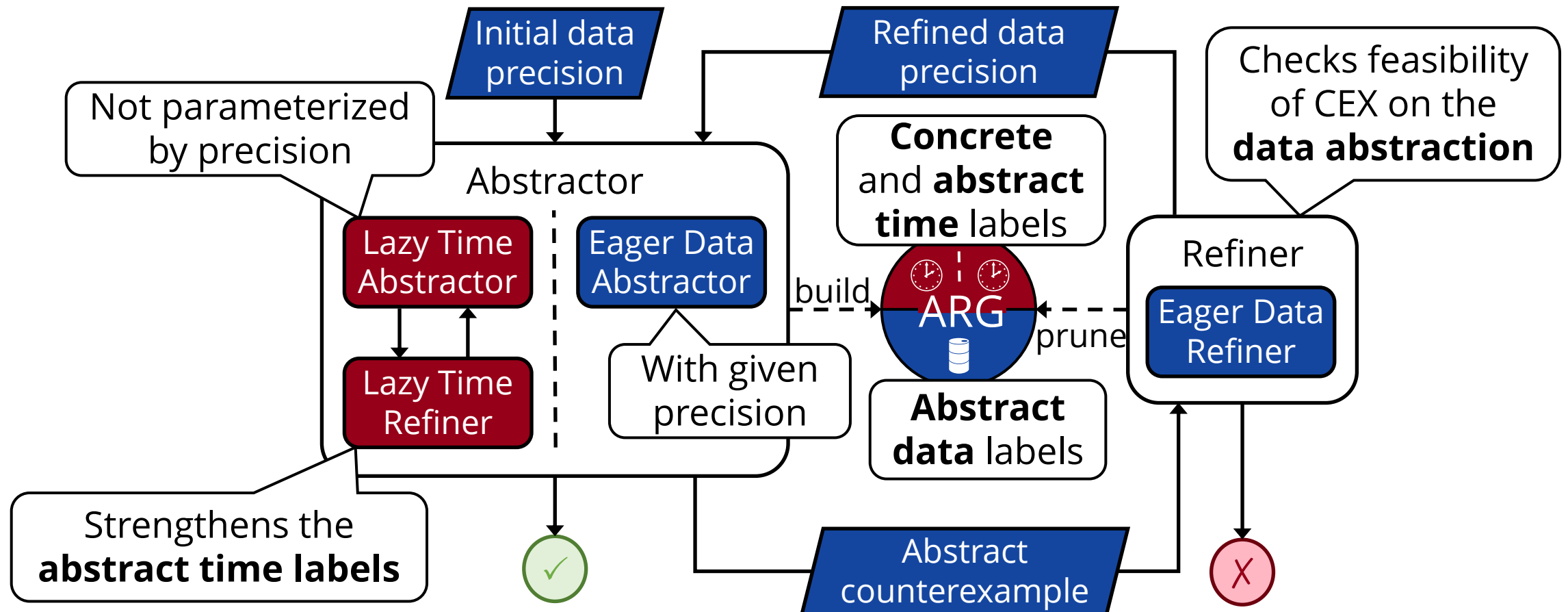
Combining CEGAR and Lazy Abstraction

CEGAR on **data** projection, **lazy abstraction** on **time** projection



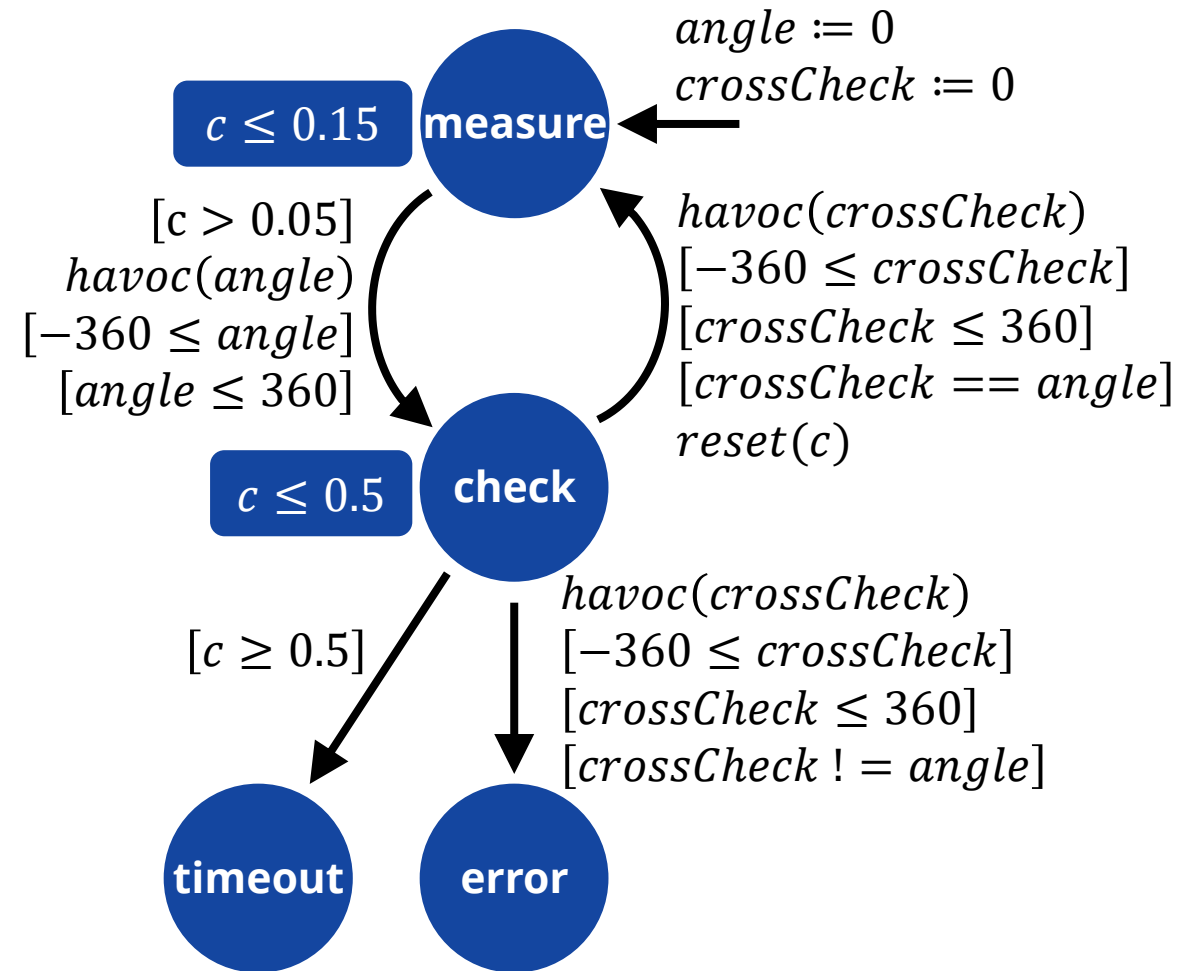
Combining CEGAR and Lazy Abstraction

CEGAR on **data** projection, **lazy abstraction** on **time** projection






Combining CEGAR and Lazy Abstraction

Running example: simplified model of redundant automotive sensor

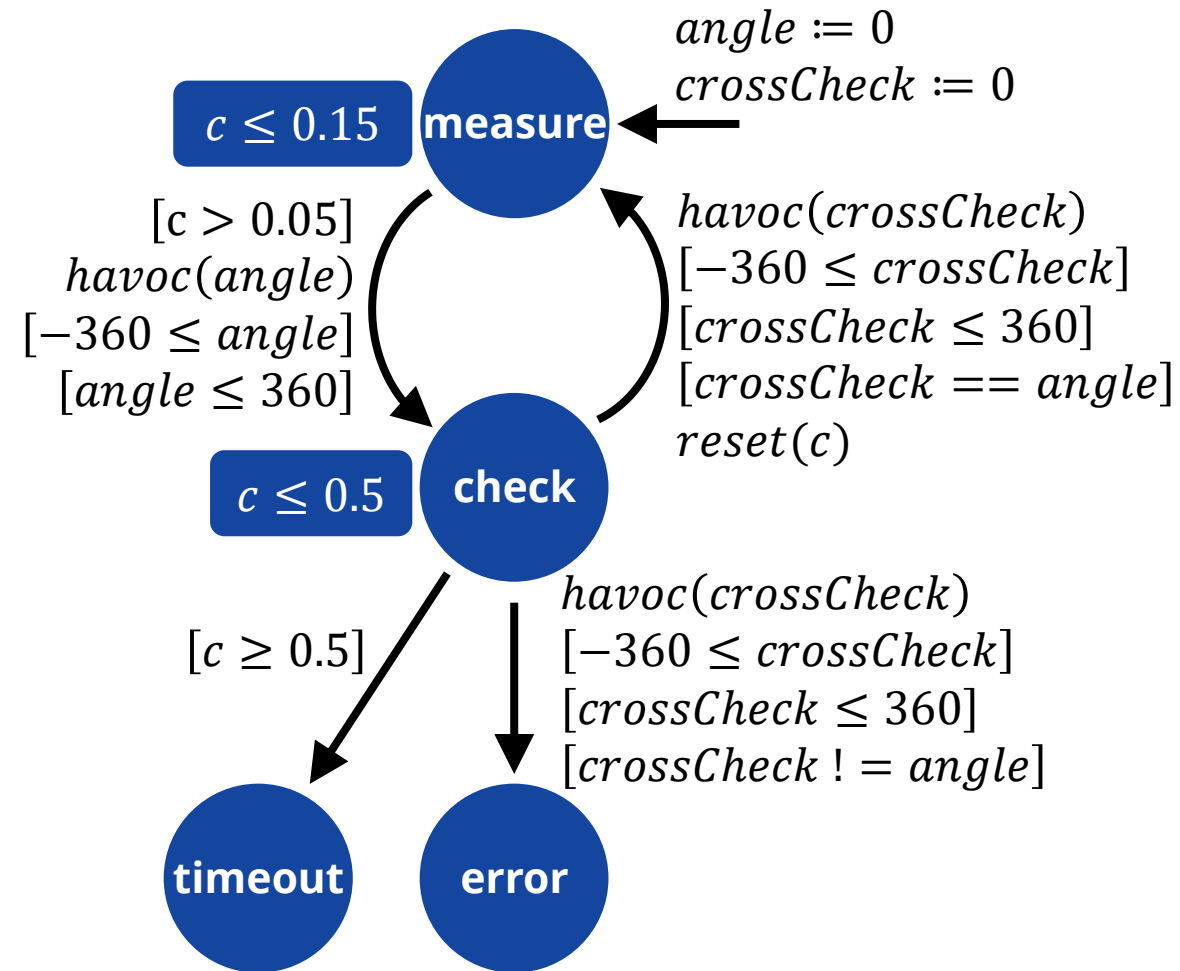


Combining CEGAR and Lazy Abstraction

Loc.	measure
	$\{p\}$
 C.	$c \geq 0$ $\wedge c \leq 0.15$
 A.	$c \geq 0$

Precision: $\pi = \{p\}$
 $p = (\text{crossCheck} == \text{angle})$

Running example: simplified model of redundant automotive sensor



Combining CEGAR and Lazy Abstraction

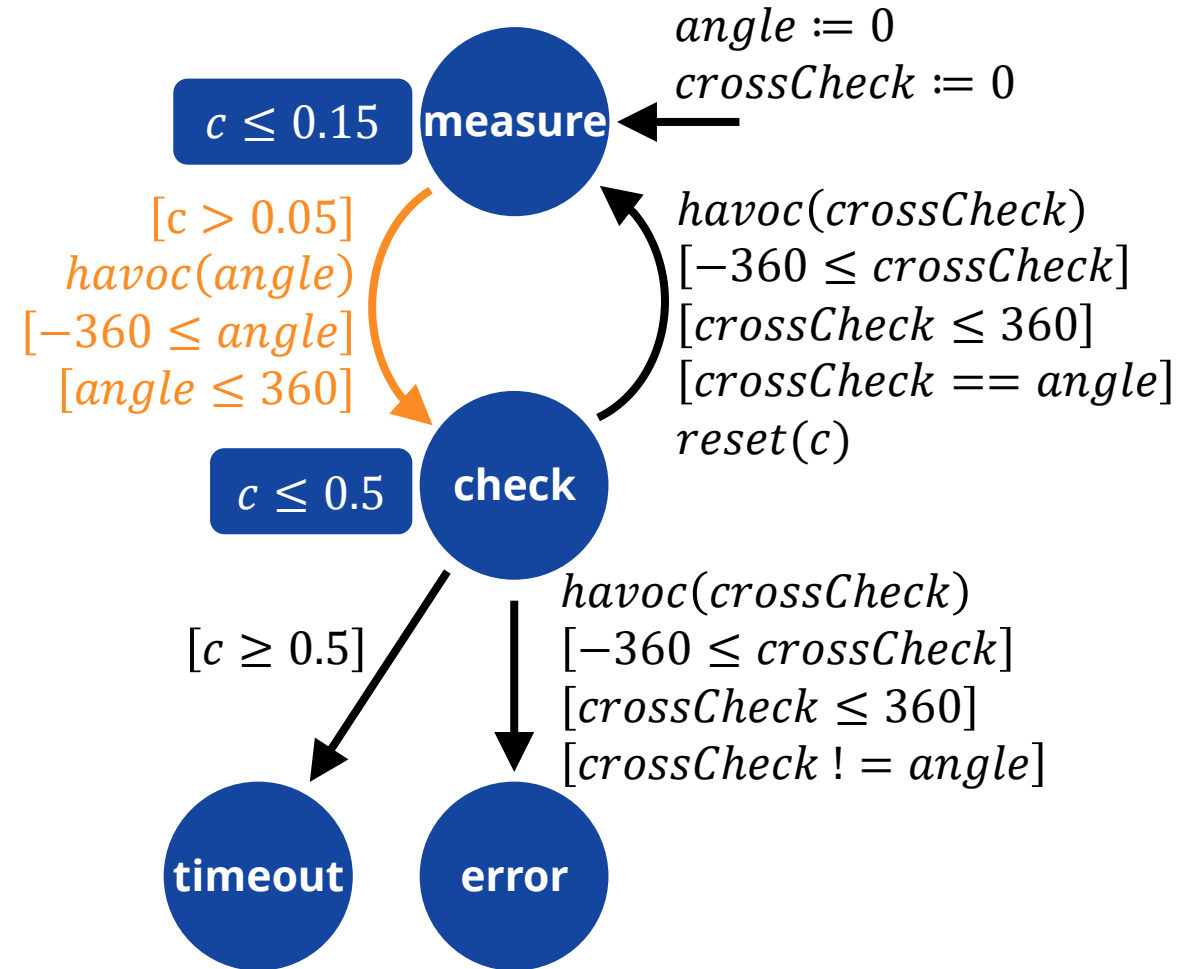
Loc.	measure
	$\{p\}$
C.	$c \geq 0$ $\wedge c \leq 0.15$
A.	$c \geq 0$

Precision: $\pi = \{p\}$
 $p = (\text{crossCheck} == \text{angle})$

Running example: simplified model of redundant automotive sensor

Loc.	check
	$\{p\}$
C.	$c > 0.05$ $\wedge c \leq 0.5$
A.	$c \geq 0$

Loc.	check
	$\{\neg p\}$
C.	$c > 0.05$ $\wedge c \leq 0.5$
A.	$c \geq 0$



Combining CEGAR and Lazy Abstraction

Precision: $\pi = \{p\}$
 $p = (\text{crossCheck} == \text{angle})$

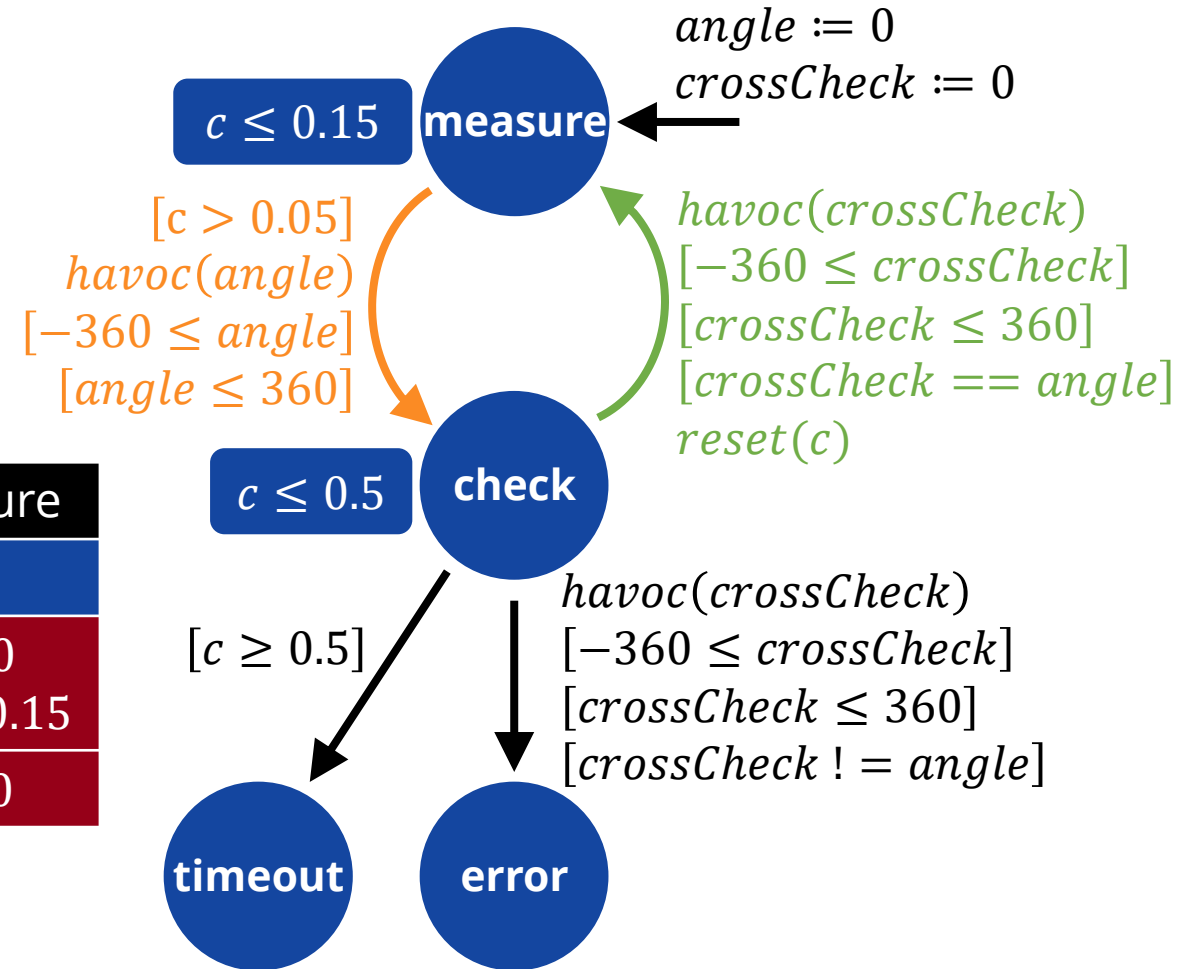
Running example: simplified model of redundant automotive sensor

Loc.	measure
	$\{p\}$
C.	$c \geq 0$ $\wedge c \leq 0.15$
A.	$c \geq 0$

Loc.	check
	$\{p\}$
C.	$c > 0.05$ $\wedge c \leq 0.5$
A.	$c \geq 0$

Loc.	check
	$\{\neg p\}$
C.	$c > 0.05$ $\wedge c \leq 0.5$
A.	$c \geq 0$

Loc.	measure
	$\{p\}$
C.	$c \geq 0$ $\wedge c \leq 0.15$
A.	$c \geq 0$



Combining CEGAR and Lazy Abstraction

Precision: $\pi = \{p\}$
 $p = (\text{crossCheck} == \text{angle})$

Running example: simplified model of redundant automotive sensor

Loc.	measure
	$\{p\}$
C.	$c \geq 0$ $\wedge c \leq 0.15$
A.	$c \geq 0$

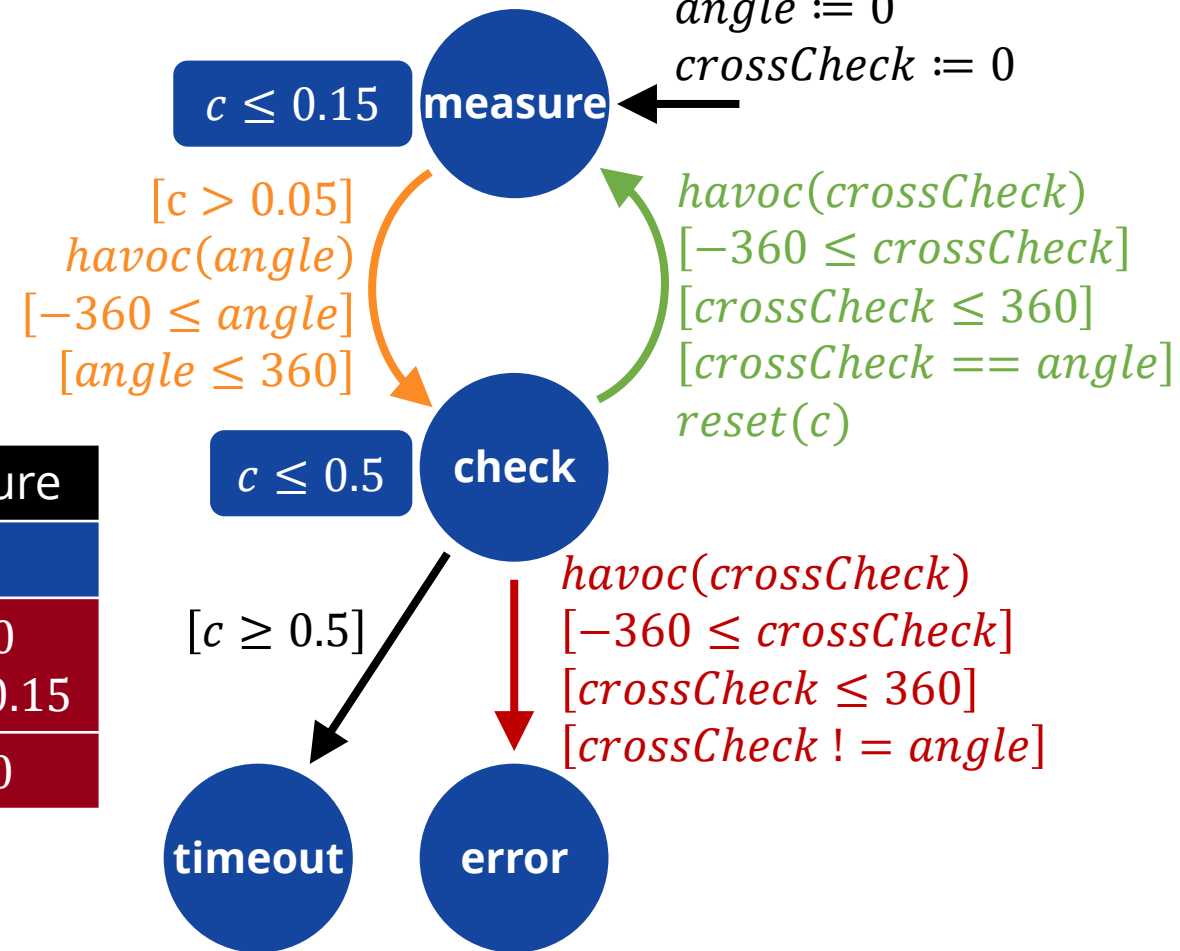
Loc.	check
	$\{p\}$
C.	$c > 0.05$ $\wedge c \leq 0.5$
A.	$c \geq 0$

Loc.	check
	$\{\neg p\}$
C.	$c > 0.05$ $\wedge c \leq 0.5$
A.	$c \geq 0$

Loc.	error
	$\{\neg p\}$
C.	$c > 0.05$
A.	$c \geq 0$

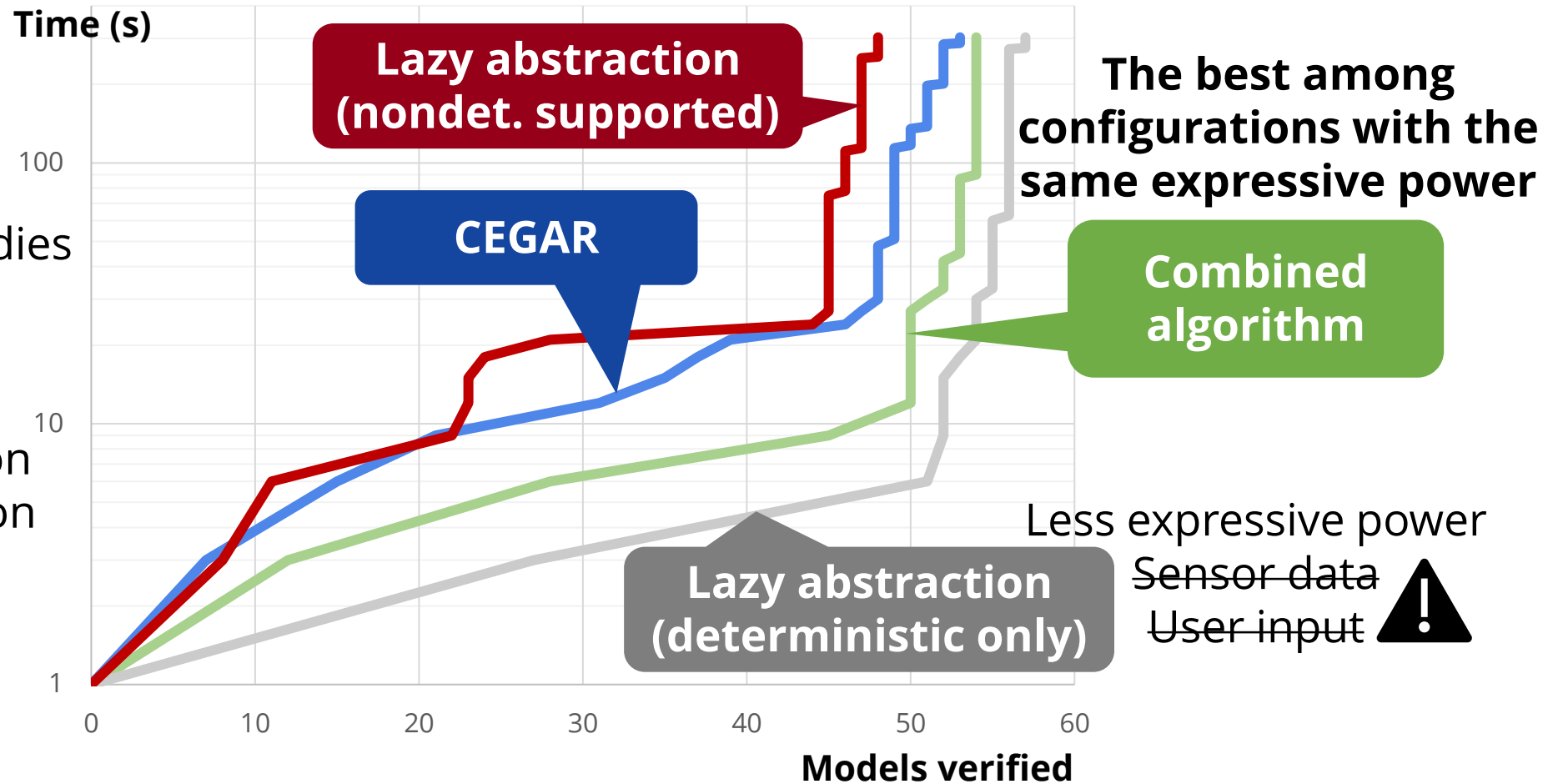
Loc.	measure
	$\{p\}$
C.	$c \geq 0$ $\wedge c \leq 0.15$
A.	$c \geq 0$

Refiner ←



Evaluation of the Combined Algorithm

- 95 XTA models
 - Synthetic models
 - Industrial case studies
- Restricted set of data operations
 - Enables comparison with lazy abstraction (det. and nondet.) and CEGAR



Summary

