Counterexample-Guided Commutativity

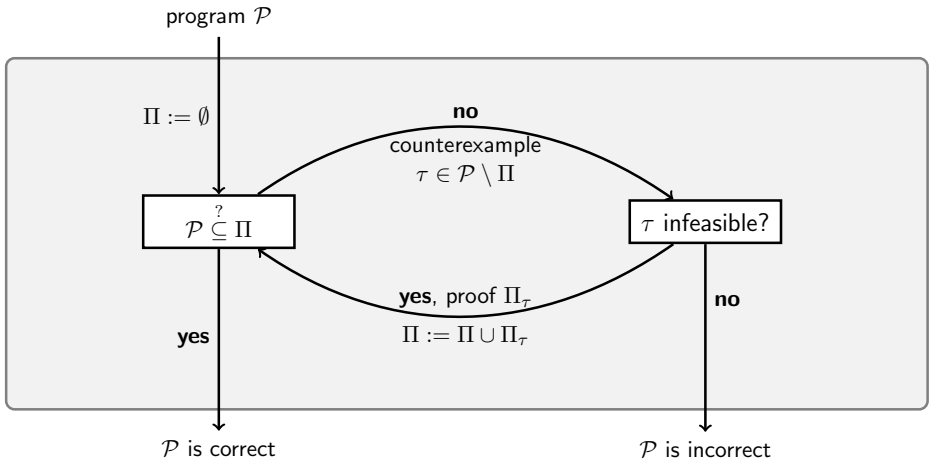
Marcel Ebbinghaus, Dominik Klumpp, Andreas Podelski

University of Freiburg

23^{rd} July 2025

CAV 2025

Counterexample-Guided Abstraction Refinement (CEGAR)



Example Program

Precondition

$size = 0 \wedge x = 5$

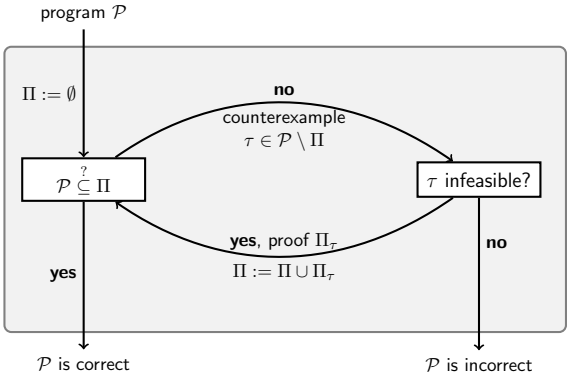
Producer (thread 1)

```
1 while (*) {
2   add(5);
3 }
```

Consumer (thread 2)

```
1 var x : int;
2 while (*) {
3   x := take();
4 }
5 assert x == 5;
```

CEGAR applied to the example



Precondition

$size = 0 \wedge x = 5$

Producer (thread 1)

```
1 while (*) {
2   add(5);
3 }
```

Consumer (thread 2)

```
1 var x : int;
2 while (*) {
3   x := take();
4 }
5 assert x == 5;
```

CEGAR applied to the example

- $\tau_1 :=$ `add(5)` `x:=take()` `x:=take()` `x!=5`

CEGAR applied to the example

- $\tau_1 :=$ `add(5)` `x:=take()` `x:=take()` `x!=5`
- Π_{τ_1} requires the predicates $\{false, size \leq 0, size \leq 1\}$

CEGAR applied to the example

- $\tau_1 :=$ `add(5)` `x:=take()` `x:=take()` `x!=5`
- Π_{τ_1} requires the predicates $\{false, size \leq 0, size \leq 1\}$
- $\tau_2 :=$ `add(5)` `add(5)` `x:=take()` `x:=take()` `x:=take()` `x!=5`

CEGAR applied to the example

- $\tau_1 :=$ `add(5)` `x:=take()` `x:=take()` `x!=5`
- Π_{τ_1} requires the predicates $\{false, size \leq 0, size \leq 1\}$
- $\tau_2 :=$ `add(5)` `add(5)` `x:=take()` `x:=take()` `x:=take()` `x!=5`
- Π_{τ_2} requires the predicates $\{false, size \leq 0, size \leq 1, size \leq 2\}$

CEGAR applied to the example

- $\tau_1 :=$ `add(5)` `x:=take()` `x:=take()` `x!=5`
- Π_{τ_1} requires the predicates $\{false, size \leq 0, size \leq 1\}$
- $\tau_2 :=$ `add(5)` `add(5)` `x:=take()` `x:=take()` `x:=take()` `x!=5`
- Π_{τ_2} requires the predicates $\{false, size \leq 0, size \leq 1, size \leq 2\}$
- Proving similar $\tau_3, \tau_4, ...$ requires additional predicates $size \leq 3, size \leq 4, ...$

CEGAR applied to the example

- $\tau_1 :=$ `add(5)` `x:=take()` `x:=take()` `x!=5`
- Π_{τ_1} requires the predicates $\{false, size \leq 0, size \leq 1\}$
- $\tau_2 :=$ `add(5)` `add(5)` `x:=take()` `x:=take()` `x:=take()` `x!=5`
- Π_{τ_2} requires the predicates $\{false, size \leq 0, size \leq 1, size \leq 2\}$
- Proving similar $\tau_3, \tau_4, ...$ requires additional predicates $size \leq 3, size \leq 4, ...$

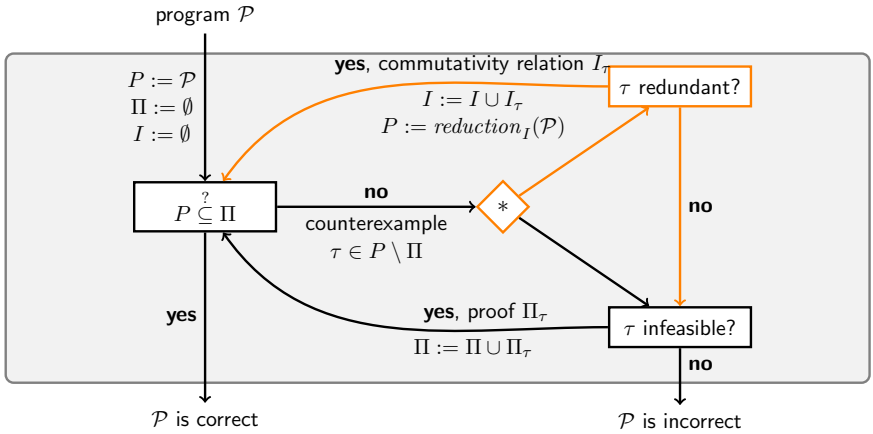
- τ of the form (`add(5)` `x:=take()`)* `x:=take()` `x!=5`

CEGAR applied to the example

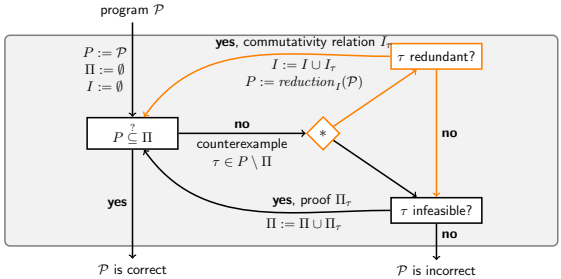
- $\tau_1 :=$ `add(5)` `x:=take()` `x:=take()` `x!=5`
- Π_{τ_1} requires the predicates $\{false, size \leq 0, size \leq 1\}$
- $\tau_2 :=$ `add(5)` `add(5)` `x:=take()` `x:=take()` `x:=take()` `x!=5`
- Π_{τ_2} requires the predicates $\{false, size \leq 0, size \leq 1, size \leq 2\}$
- Proving similar $\tau_3, \tau_4, ...$ requires additional predicates $size \leq 3, size \leq 4, ...$

- τ of the form (`add(5)` `x:=take()`)* `x:=take()` `x!=5`
- Commutativity, but Counterexample-Guided!

CEGAR+CC

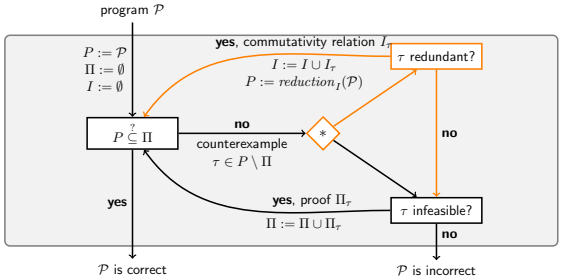

program $\mathcal{P}$
$P := \mathcal{P}$
$\Pi := \emptyset$
$I := \emptyset$
$P \overset{?}{\subseteq} \Pi$
yes
$\mathcal{P}$ is correct
no
counterexample
$\tau \in P \setminus \Pi$
*
yes, commutativity relation I_τ
$I := I \cup I_\tau$
$P := reduction_I(\mathcal{P})$
τ redundant?
no
yes, proof Π_τ
$\Pi := \Pi \cup \Pi_\tau$
τ infeasible?
no
$\mathcal{P}$ is incorrect

CEGAR+CC



How do we prove that τ is redundant?

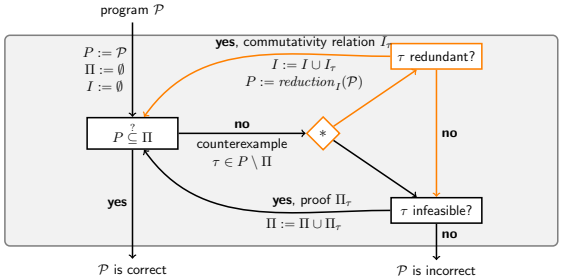
CEGAR+CC



How do we prove that τ is redundant?

- Step I: Find a commutativity relation I_τ s.t. $\tau \notin reduction_{I \cup I_\tau}(\mathcal{P})$.

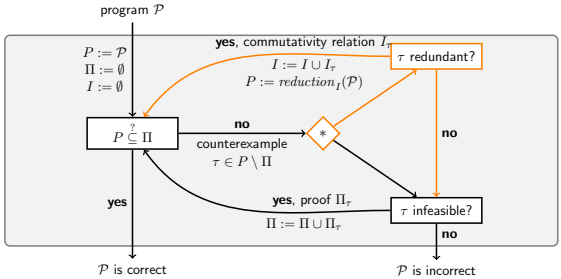
CEGAR+CC



How do we prove that τ is redundant?

- Step I: Find a commutativity relation I_τ s.t. $\tau \notin reduction_{I \cup I_\tau}(\mathcal{P})$.
- Step II: Prove that I_τ is sound.

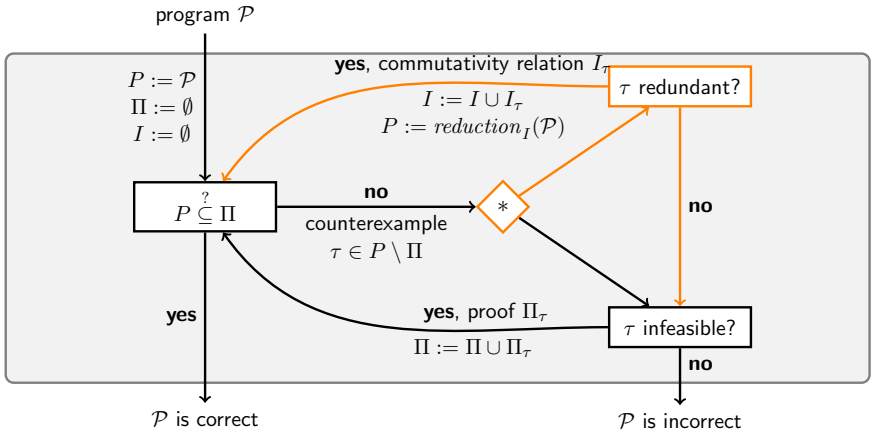
CEGAR+CC



How do we prove that τ is redundant?

- Step I: Find a commutativity relation I_τ s.t. $\tau \notin reduction_{I \cup I_\tau}(\mathcal{P})$.
- Step II: Prove that I_τ is sound.
- Step III: Generalize I_τ to prove the redundancy of an infinite super-set of $\{\tau\}$.

CEGAR+CC


program $\mathcal{P}$
$P := \mathcal{P}$
$\Pi := \emptyset$
$I := \emptyset$
$P \overset{?}{\subseteq} \Pi$
yes
$\mathcal{P}$ is correct
no
counterexample
$\tau \in P \setminus \Pi$
*
yes, commutativity relation I_τ
$I := I \cup I_\tau$
$P := reduction_I(\mathcal{P})$
τ redundant?
no
yes, proof Π_τ
$\Pi := \Pi \cup \Pi_\tau$
τ infeasible?
no
$\mathcal{P}$ is incorrect

Evaluation

- CEGAR+CC implemented in ULTIMATE GEMCUTTER[a].
- Weaver benchmarks[b] consisting of 183 programs.

[a] github.com/ultimate-pa/ultimate
[b] github.com/weaver-verifier/weaver/tree/master/examples

Evaluation

- CEGAR+CC implemented in ULTIMATE GEMCUTTER[a].
- Weaver benchmarks[b] consisting of 183 programs.

[a] github.com/ultimate-pa/ultimate
[b] github.com/weaver-verifier/weaver/tree/master/examples

	context-insensitive	proof-sensitive	CEGAR+CC	
			sufficient	nec. & sufficient
# successful tasks	96	99	109	111
comm. refinements	N/A	N/A	15	19