Completeness Thresholds for Memory Safety
Unbounded Guarantees Via Bounded Proofs

Tobias Reinhard, Justus Fasse, Bart Jacobs

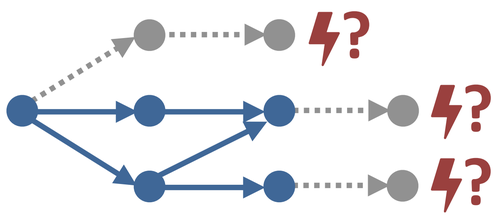
Can We Trust Bounded Proofs?

Bounded Proofs

- Prove bounded program spec

$$\vDash \forall x < 10.\ Spec$$

- Cover finite prefix of state space

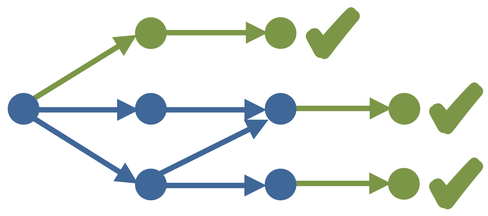


Unbounded Proofs

- Prove unbounded program spec

$$\vDash \forall x\,.\ Spec$$

- Cover entire infinite state space

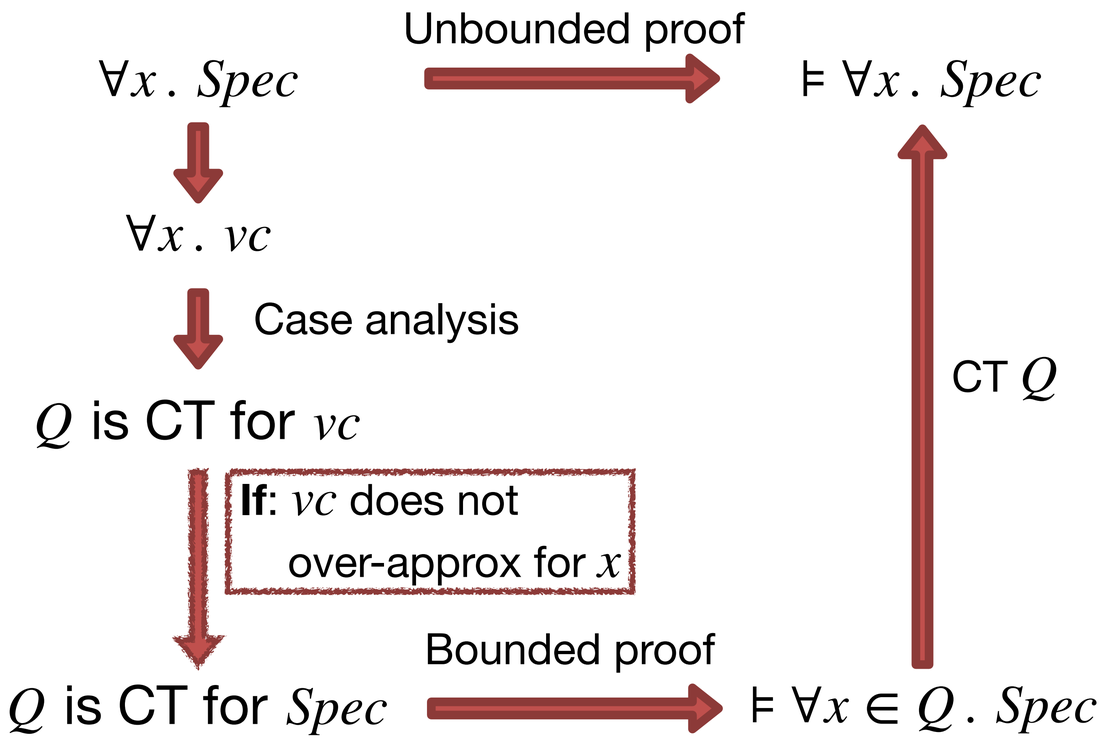


Completeness Thresholds

- **Def:** Subdomain $Q \subseteq X$ is a ***CT*** if big enough to cover all critical cases, i.e.:

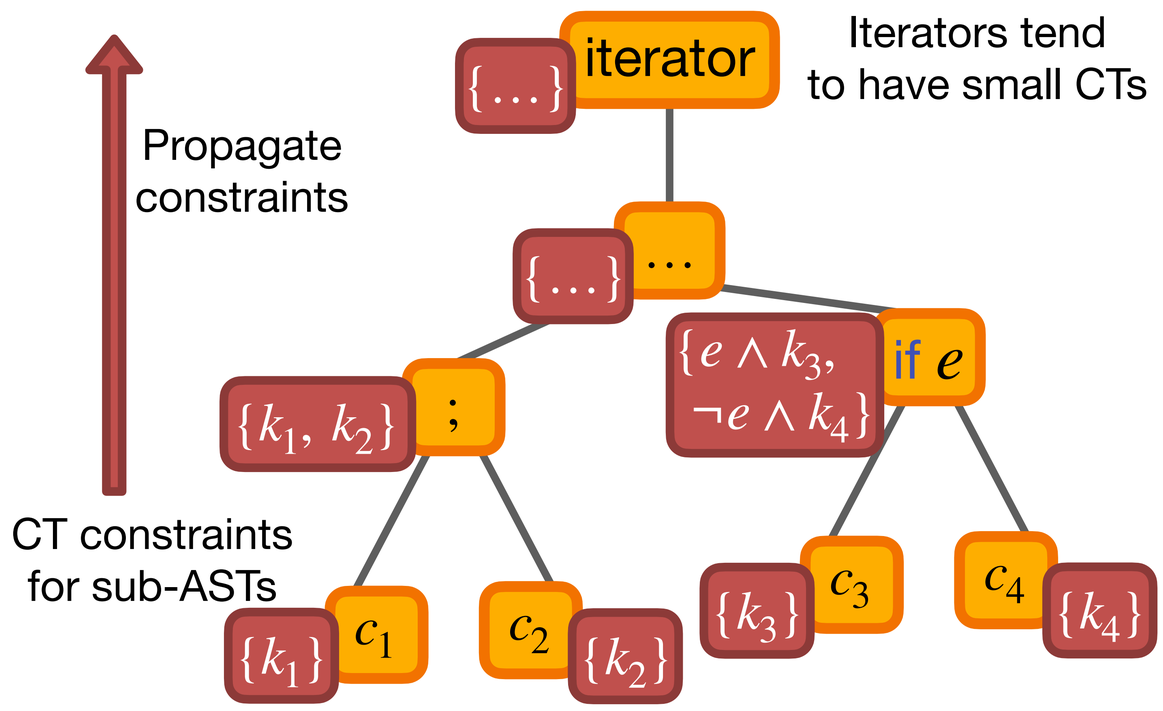
$$\vDash \forall x \in Q\,.\ Spec \quad \Rightarrow \quad \vDash \forall x \in X\,.\ Spec$$

Verification Condition Analysis



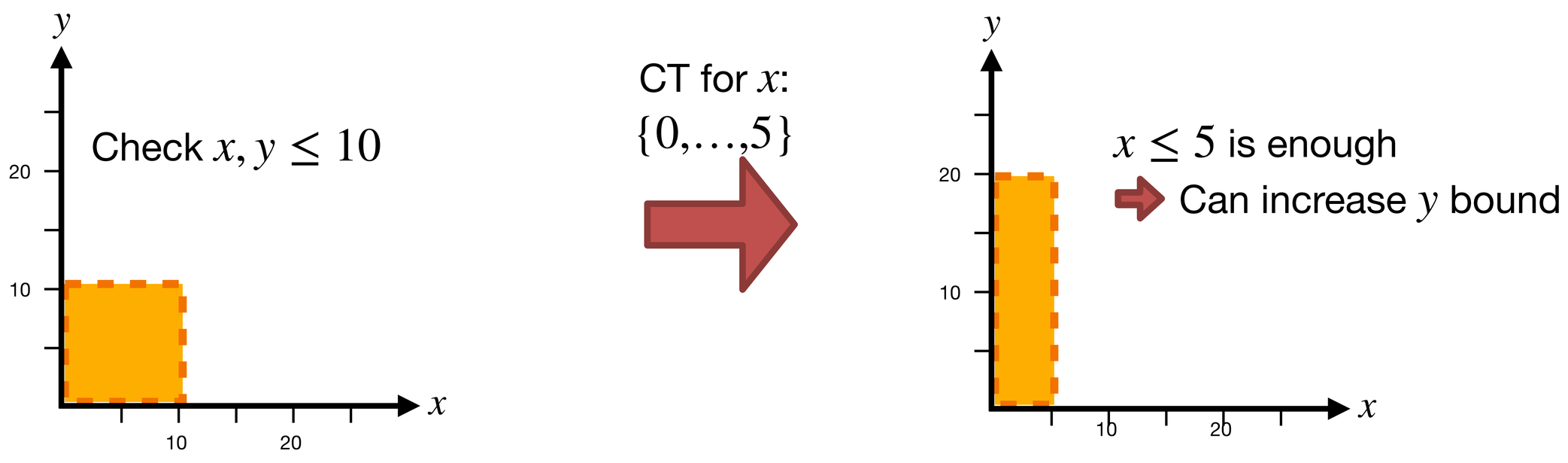
- Cases reflected in verification condition

Memory Safety CTs Compose



- CTs for disjoint inputs compose trivially

Increase Trust in Bounded Model Checking



[1] Reinhard, Fasse, Jacobs. 2023. *Completeness Thresholds for Memory Safety of Array Traversing Programs*. SOAP.
[2] Reinhard, Fasse, Jacobs. 2023. *Completeness Thresholds for Memory Safety: Unbounded Guarantees via Bounded Proofs*. arXiv.