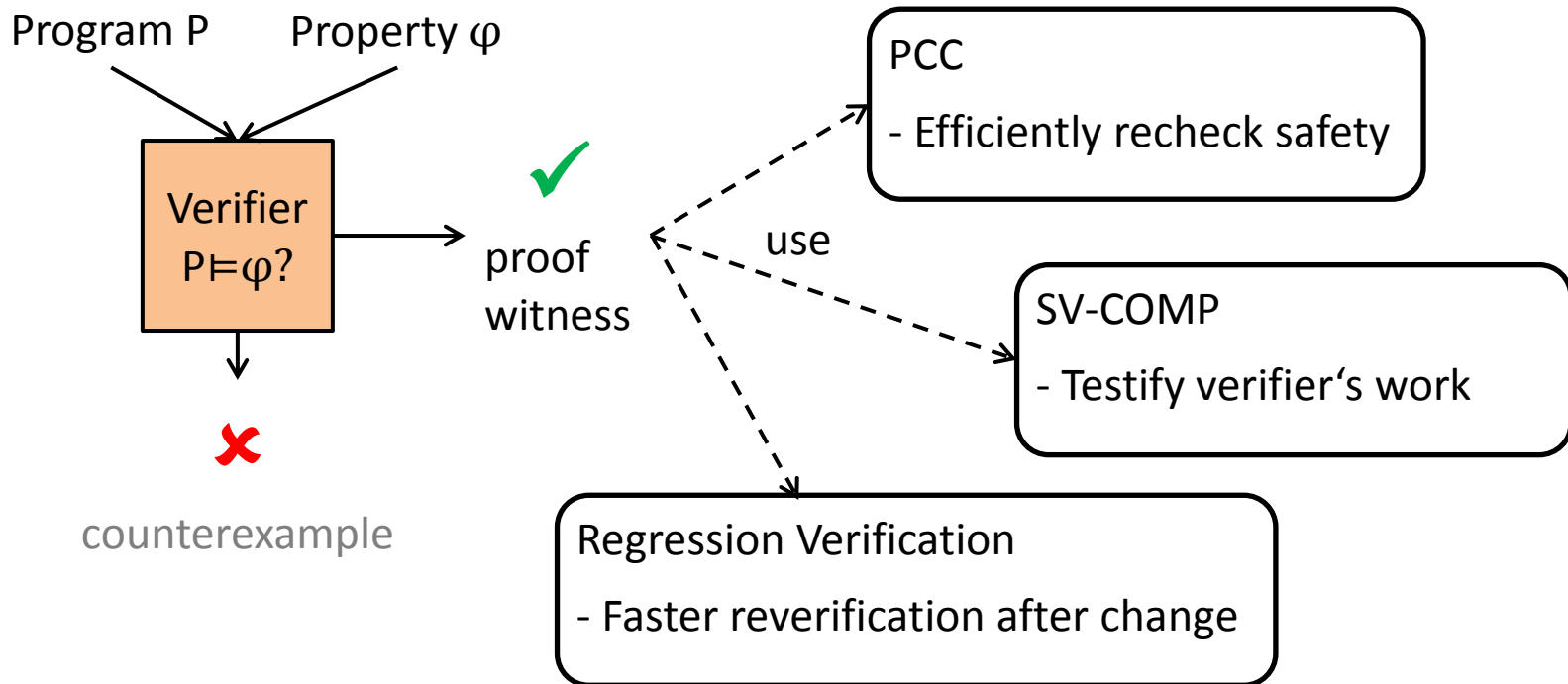


PART_{PW}

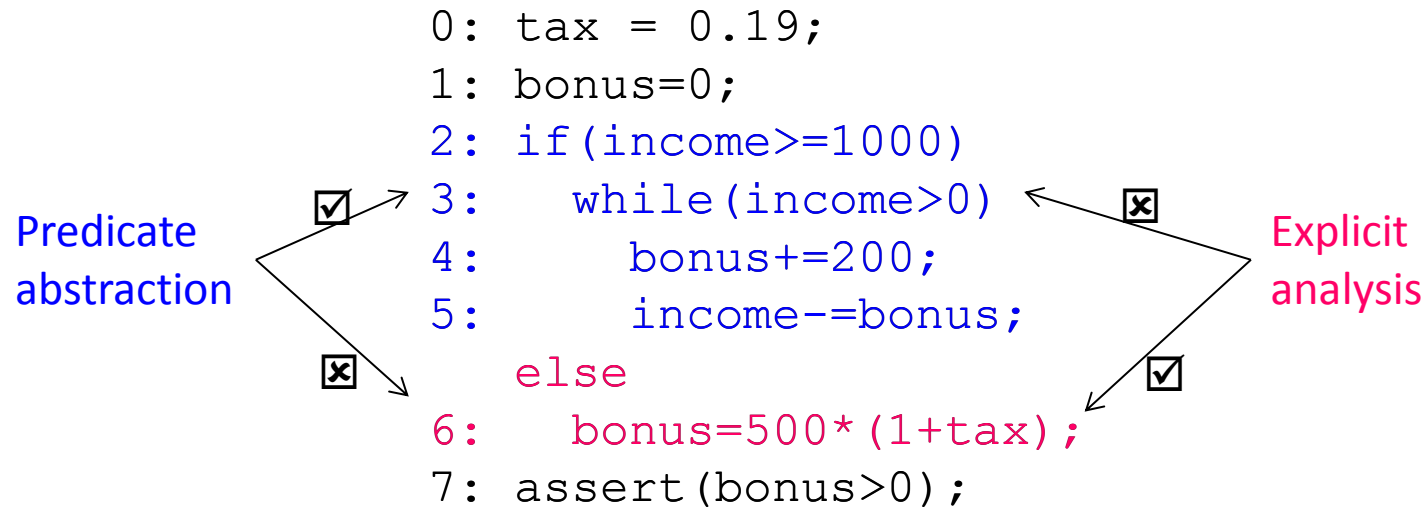
From Partial Analysis Results to a Proof Witness

Marie-Christine Jakobs

Use Cases for Proof Witnesses



Problem: Complementary Analyses



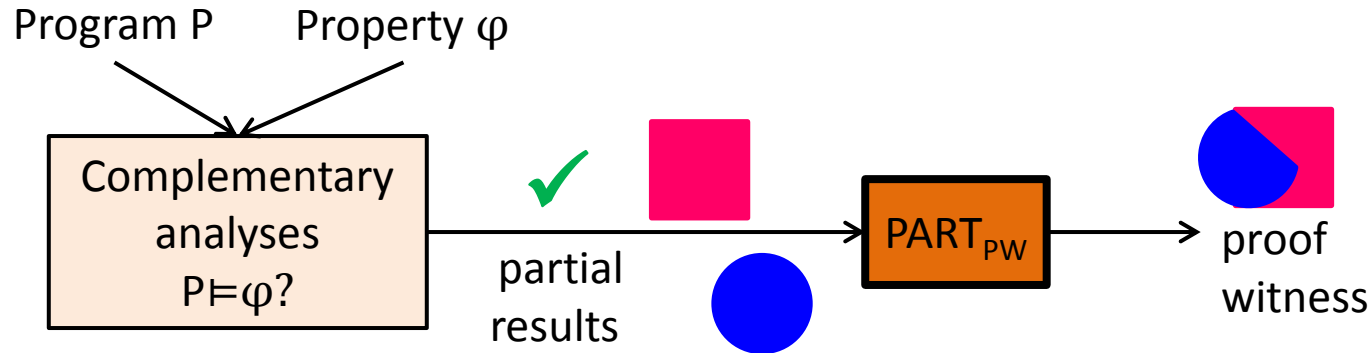
if branch: verify with predicate abstraction

else branch: verify with explicit analysis

→ 2 partial analysis results



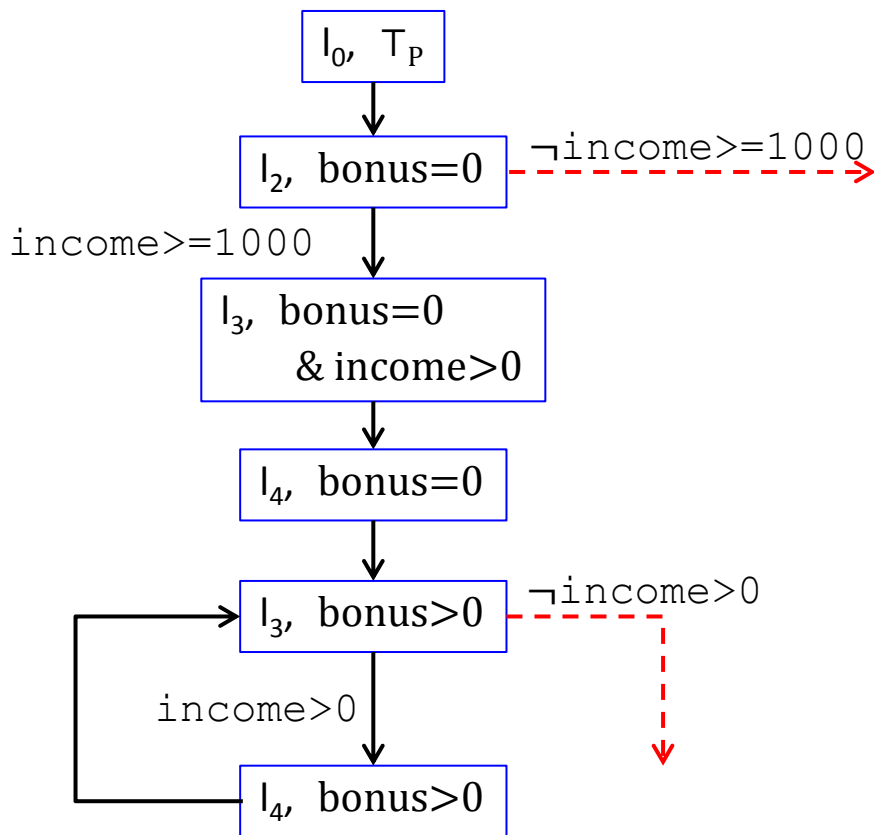
The PART_{PW} Solution



- Benefits
 - Reuse of existing proof witness approaches
 - Complex analysis hidden from witness checker

(Partial) Proof Witnesses

Here: in form of abstract reachability graphs



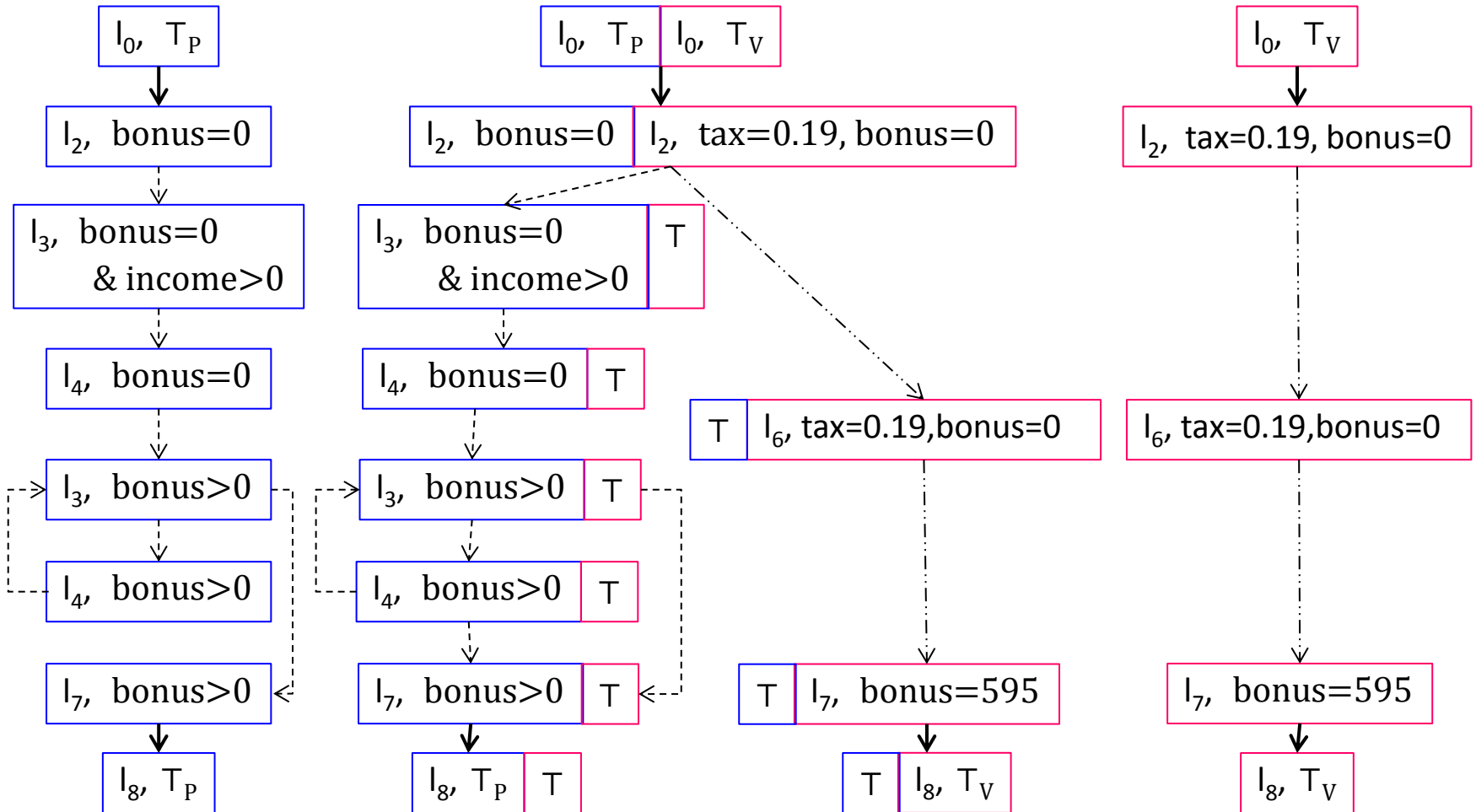
Valid Partial Proof Witness

- Root covers the initial states
- For each node, statement either
 - a) Abstract successors covered
 - b) No successors for statement
- Safe

Valid Proof Witness

- Valid partial proof witness,
- but no missing successors

An ARG from a Set of Partial ARGs



Theoretical Result

Goal: Part_{PW} constructs valid proof witnesses

Require: Partial ARGs must cover all execution paths

→ Use complete set of partial ARGs (stronger, abstraction based)

Theorem (proven)

- Let S_{pARG} be complete set of partial ARGs.
Then, $\text{Part}_{\text{PW}}(S_{\text{pARG}})$ is a valid proof witness.

Experiments

Questions

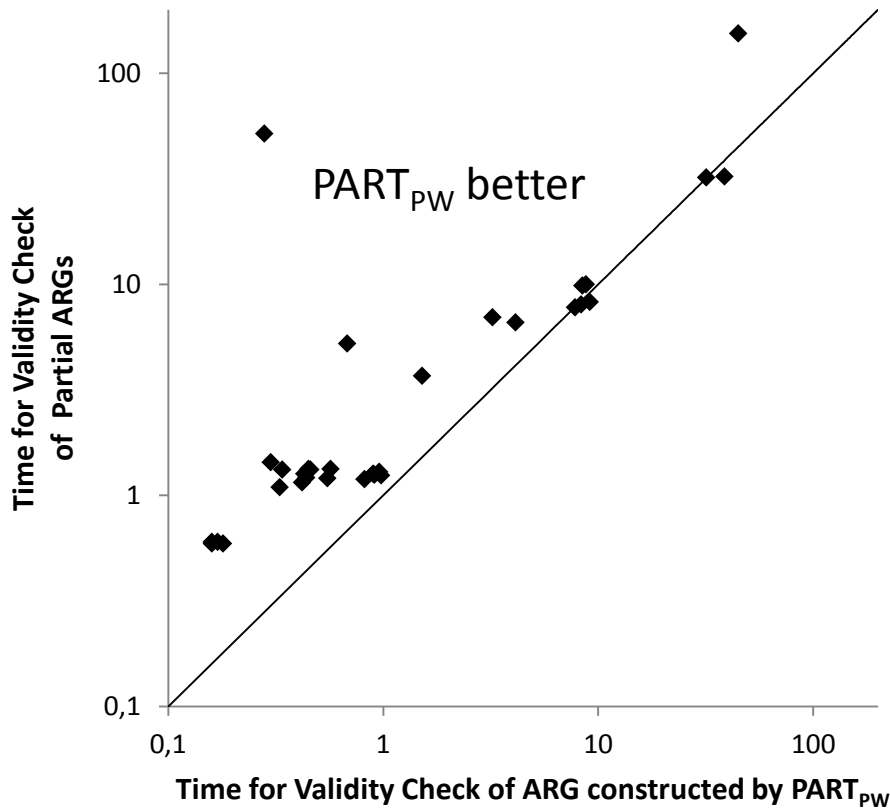
1. Is Part_{PW} + standard witness approach better than checking set of partial ARGs?
2. Is Part_{PW} + standard witness approach better than verification?
3. How costly is Part_{PW} ?

Set Up

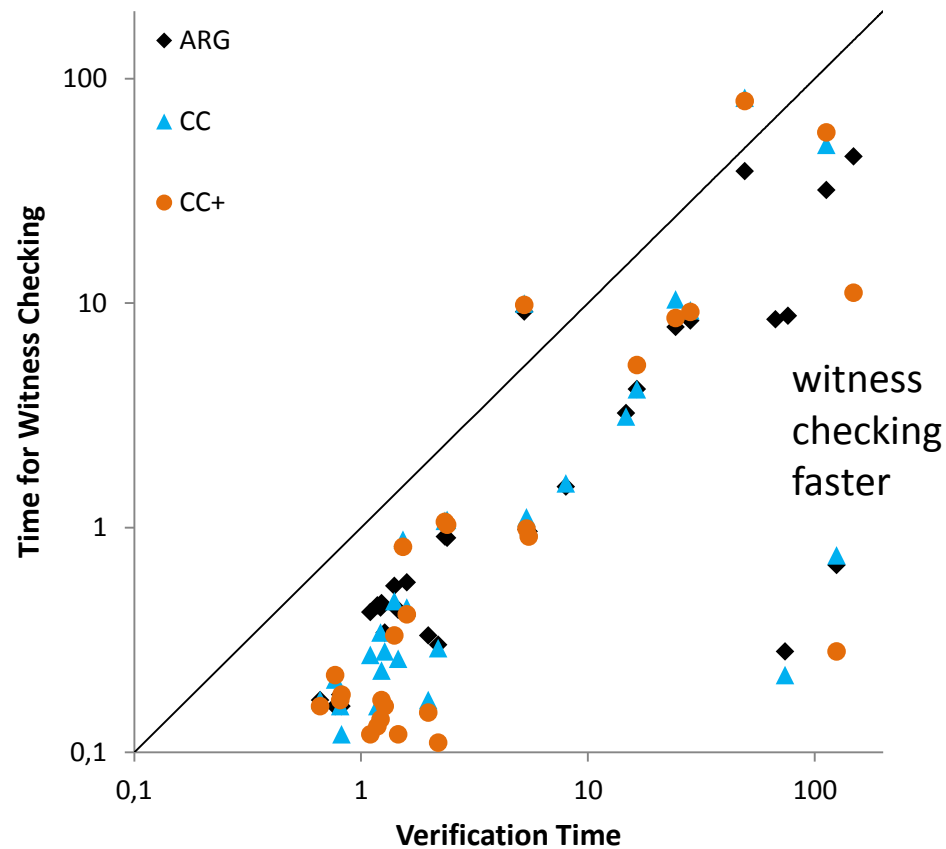
- Construction of Partial ARGs
 - Conditional model checking^[1]
 - Different combinations
 - Restrict to tasks for which combinations beneficial
- Witness Approaches
 - ARG as witness
 - ARG nodes as witness
 - Structured subset of ARG nodes as witness
 - Set of partial ARGs as witness

[1] Beyer et al., Conditional model checking: a technique to pass information between verifiers, FSE, 2012.

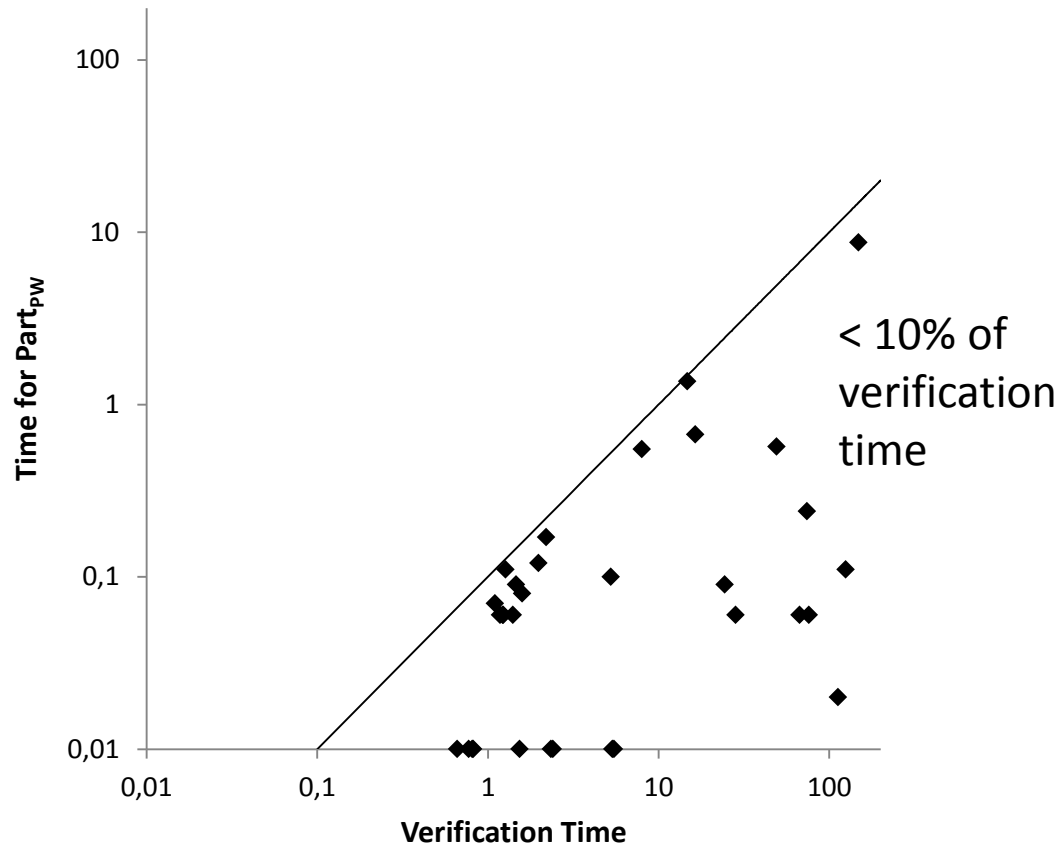
Q1: PART_{PW} vs. Specific Solution



Q2: Witness Checking vs. Verification

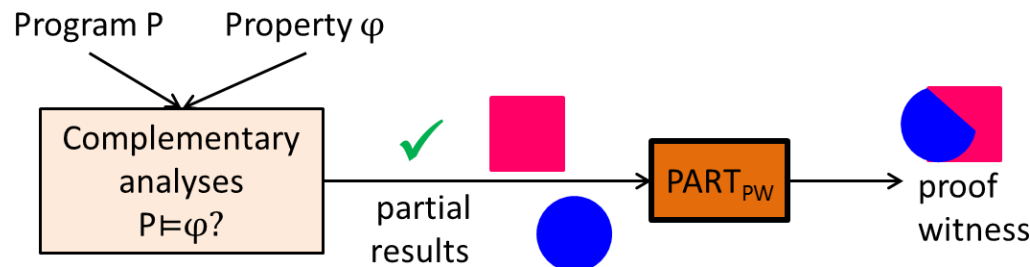


Q3: Overhead of Part_{PW}



Conclusion

- Technique PART_{PW}



- Provably constructs valid proof witnesses
- Experiments
 - Seamless integration into existing approaches
 - More efficient than specific solution
 - PART_{PW} overhead small