PART\textsubscript{PW}

From Partial Analysis Results to a Proof Witness

Marie-Christine Jakobs
Use Cases for Proof Witnesses

Program P \rightarrow Property \varphi \Rightarrow \text{Verifier} \Rightarrow \text{proof witness} \Rightarrow \text{PCC}
- Efficiently recheck safety
- SV-COMP
  - Testify verifier’s work

\text{Regression Verification}
- Faster reverification after change

\text{counterexample}
Problem: Complementary Analyses

if branch: verify with predicate abstraction
else branch: verify with explicit analysis

→ 2 partial analysis results
The \( \text{PART}_{PW} \) 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

\[ l_0, \top \]
\[ l_2, \text{bonus}=0 \]
\[ l_3, \text{bonus}=0 \]
\[ l_4, \text{bonus}=0 \]
\[ \rightarrow l_3, \text{bonus}>0 \]
\[ l_4, \text{bonus}>0 \]
\[ l_7, \text{bonus}>0 \]
\[ l_8, \top \]
\[ l_0, \top \]
\[ l_2, \text{bonus}=0 \]
\[ l_2, \text{tax}=0.19, \text{bonus}=0 \]
\[ l_3, \text{bonus}=0 \]
\[ l_3, \text{bonius}=0 \]
\[ l_4, \text{bonus}=0 \]
\[ l_4, \text{bonus}=0 \]
\[ \rightarrow l_3, \text{bonus}>0 \]
\[ l_4, \text{bonus}>0 \]
\[ l_7, \text{bonus}>0 \]
\[ l_8, \top \]
\[ l_0, \top \]
\[ l_0, \top \]
\[ l_0, \top \]
\[ l_2, \text{tax}=0.19, \text{bonus}=0 \]
\[ l_3, \text{bonus}=0 \]
\[ l_3, \text{bonus}=0 \]
\[ l_4, \text{bonus}=0 \]
\[ l_4, \text{bonus}=0 \]
\[ \rightarrow l_3, \text{bonus}>0 \]
\[ l_4, \text{bonus}>0 \]
\[ l_7, \text{bonus}>0 \]
\[ l_8, \top \]
\[ l_6, \text{tax}=0.19, \text{bonus}=0 \]
\[ l_7, \text{bonius}=595 \]
\[ l_8, \top \]
\[ l_6, \text{tax}=0.19, \text{bonus}=0 \]
\[ l_7, \text{bonus}=595 \]
\[ l_8, \top \]
Theoretical Result

**Goal:** Part\textsubscript{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, $\text{Part}_{PW}(S_{pARG})$ is a valid proof witness.
Experiments

Questions
1. Is $\text{Part}_{PW} + \text{standard witness approach}$ better than checking set of partial ARGs?

2. Is $\text{Part}_{PW} + \text{standard witness approach}$ better than verification?

3. How costly is $\text{Part}_{PW}$?

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

Q1: PART\textsubscript{PW} vs. Specific Solution

![Graph showing comparison between PART\textsubscript{PW} and Specific Solution]
Q2: Witness Checking vs. Verification

The diagram compares the time for witness checking against verification time for three different methods: ARG, CC, and CC+. The graph shows that the time for witness checking is generally faster than the verification time, with the points falling below the diagonal line that represents equal times for both tasks.
Q3: Overhead of Part$_{PW}$

< 10% of verification time
Conclusion

• Technique $\text{PART}_{PW}$
  - Provably constructs valid proof witnesses

• Experiments
  - Seamless integration into existing approaches
  - More efficient than specific solution
  - $\text{PART}_{PW}$ overhead small