Satisfiability-Preserving Reasoning in Software Verification

Adrián Rebola-Pardo (TU Wien)

FMCAD 2017
Vienna, Austria
October 4th, 2017
Supported by FWF W1255-N23 and Microsoft Research
Craig interpolants $A \land B$ unsatisfiable
Interpolation for model checking

Craig interpolants \( A \land B \) unsatisfiable

- \( A \models P \)
- \( P \land B \) is unsatisfiable
- \( \text{var}(P) \subseteq \text{var}(A) \cap \text{var}(B) \)
Craig interpolants  \( A \land B \) unsatisfiable
- \( A \models P \)
- \( P \land B \) is unsatisfiable
- \( \text{var}(P) \subseteq \text{var}(A) \cap \text{var}(B) \)

Interpolant-based model checking
- Interpolants help us avoid state space blow-up
- Complete, unbounded model checking through SAT solving is attained
Interpolant generation

The good old times

unsatisfiable CNF instance → SAT solver → resolution proof → interpolation system → interpolant
Interpolant generation

The good old times

unsatisfiable CNF instance \(\xrightarrow{\text{SAT solver}}\) resolution proof \(\xrightarrow{\text{interpolation system}}\) interpolant

Interpolant generation from resolution proofs

The induction invariant of this recursion depends strongly on soundness.
Interpolant generation

The good old times

unsatisfiable CNF instance $\rightarrow$ SAT solver $\rightarrow$ resolution proof $\rightarrow$ interpolation system $\rightarrow$ interpolant

Interpolant generation from resolution proofs

The induction invariant of this recursion depends strongly on soundness.
Interpolant generation

The good old times

unsatisfiable CNF instance $\xrightarrow{\text{SAT solver}}$ resolution proof $\xrightarrow{\text{interpolation system}}$ interpolant

Interpolant generation from resolution proofs

The induction invariant of this recursion depends strongly on soundness.
Interpolant generation

The good old times

unsatisfiable CNF instance \(\rightarrow\) SAT solver \(\rightarrow\) resolution proof \(\rightarrow\) interpolation system \(\rightarrow\) interpolant

Interpolant generation from resolution proofs

The induction invariant of this recursion depends strongly on soundness.
The good old times are gone

Inprocessing techniques and DRAT proofs
Interpolant generation

The good old times are gone

Inprocessing techniques and DRAT proofs

- Inprocessing techniques cannot be expressed by resolution proofs.
The good old times are gone

interpolant generation

inprocessing

unsatisfiable CNF instance → SAT solver → DRAT proof → ? → interpolant

Inprocessing techniques and DRAT proofs

- Inprocessing techniques cannot be expressed by resolution proofs.
- No interpolation system is known for DRAT proofs.
Interpolant generation

The good old times are gone

Inprocessing techniques and DRAT proofs
- Inprocessing techniques cannot be expressed by resolution proofs.
- No interpolation system is known for DRAT proofs.
- DRAT proofs can derive clauses that are not implied.
Some invariants seem to be preserved...
Some invariants seem to be preserved...
DRAT proofs

RAT, not a consequence

Some invariants seem to be preserved...
Some invariants seem to be preserved...
Some invariantseemsto be preserved...
Some invariants seem to be preserved...
DRAT proofs

Some invariants seem to be preserved...

RAT, not a consequence

not a RAT, not a consequence
Some invariants seem to be preserved...
Some \textit{invariant} seems to be preserved...
Some invariant seems to be preserved... resolution consequence

[Philipp, Rebola-Pardo: LPAR ’17]
Some invariant seems to be preserved...

resolution consequence 

[Philipp, Rebola-Pardo: LPAR ’17]
Some invariant seems to be preserved...

resolution consequence  [Philipp, Rebola-Pardo: LPAR ’17]
Some invariant seems to be preserved... resolution consequence  

[Philipp, Rebola-Pardo: LPAR ’17]
Idea: convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]
Interpolation from DRAT proofs

Idea: convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

RAT elimination

RC upon \( l \)

RC upon \( l \)

consequence!

resolution upon \( l \)
Interpolation from DRAT proofs

Idea  convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

RAT elimination
Interpolation from DRAT proofs

Idea: convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

RAT elimination

Good news: an interpolant can be generated from a resolution proof.

Bad news: converting DRAT proofs to resolution proofs is exponential...
Interpolation from DRAT proofs

Idea: convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

RAT elimination

Good news: an interpolant can be generated from a resolution proof.
Bad news: converting DRAT proofs to resolution proofs is exponential...
Interpolation from DRAT proofs

Idea  convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

RAT elimination
Interpolation from DRAT proofs

Idea convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

RAT elimination

-resolution upon $l$

RC upon $l$

RC upon $l$

consequence!
**Interpolation from DRAT proofs**

**Idea** convert DRAT proofs to resolution proofs  
*Rebola-Pardo, Weissenbacher: manuscript*

**RAT elimination**

**Good news** an interpolant can be generated from a resolution proof
Interpolation from DRAT proofs

Idea: convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

RAT elimination

Good news: an interpolant can be generated from a resolution proof

Bad news: converting DRAT proofs to resolution proofs is exponential...