TU WIEN TECHNISCHE UNIVERSITÄT WIEN Vienna University of Technology

logics Logical Methods in Computer Science

Microsoft

Satisfiability-Preserving Reasoning in Software Verification

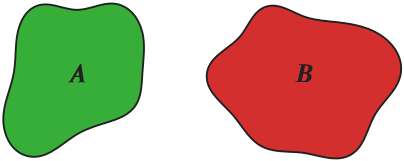
Adrián Rebola-Pardo (TU Wien)

FMCAD 2017
Vienna, Austria
October 4th, 2017

Supported by FWF W1255-N23 and Microsoft Research

Interpolation for model checking

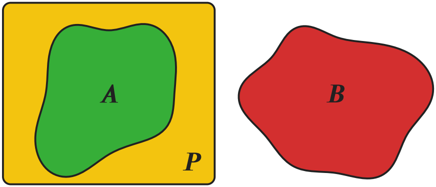
Craig interpolants $A \wedge B$ unsatisfiable



Interpolation for model checking

Craig interpolants $A \wedge B$ unsatisfiable

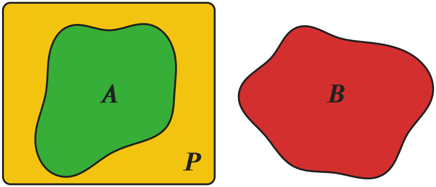
- $A \models P$
- $P \wedge B$ is unsatisfiable
- $\mathrm{var}(P) \subseteq \mathrm{var}(A) \cap \mathrm{var}(B)$



Interpolation for model checking

Craig interpolants $A \wedge B$ unsatisfiable

- $A \models P$
- $P \wedge B$ is unsatisfiable
- $\mathrm{var}(P) \subseteq \mathrm{var}(A) \cap \mathrm{var}(B)$

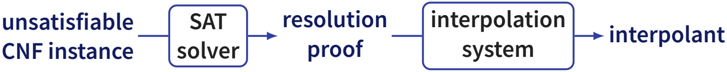


Interpolant-based model checking

- 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

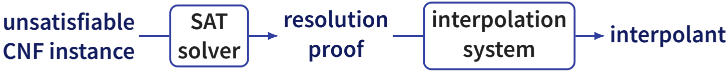
resolution proof

interpolation system

interpolant

Interpolant generation

The good old times



unsatisfiable CNF instance

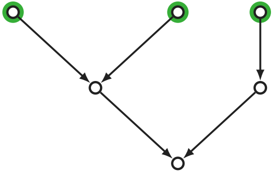
SAT solver

resolution proof

interpolation system

interpolant

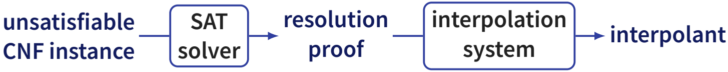
Interpolant generation from resolution proofs



The induction invariant of this recursion depends strongly on soundness.

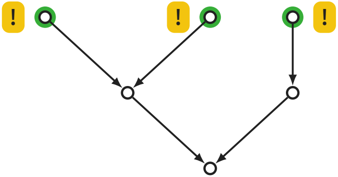
Interpolant generation

The good old times



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

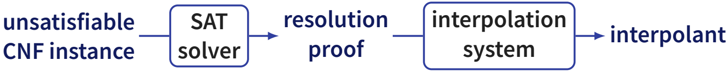
Interpolant generation from resolution proofs



The induction invariant of this recursion depends strongly on soundness.

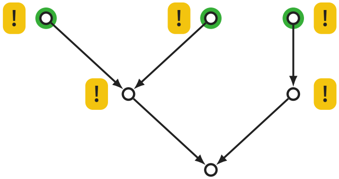
Interpolant generation

The good old times



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

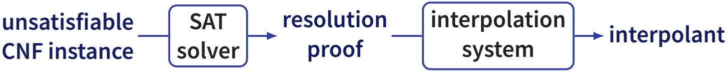
Interpolant generation from resolution proofs



The induction invariant of this recursion depends strongly on soundness.

Interpolant generation

The good old times



unsatisfiable CNF instance

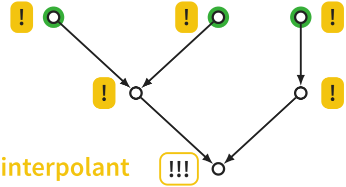
SAT solver

resolution proof

interpolation system

interpolant

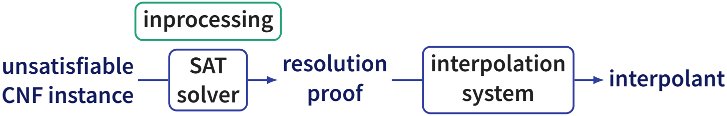
Interpolant generation from resolution proofs



The induction invariant of this recursion depends strongly on soundness.

Interpolant generation

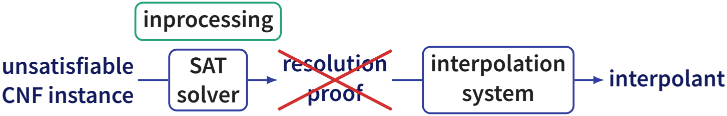
The good old times are gone



Inprocessing techniques and DRAT proofs

Interpolant generation

The good old times are gone

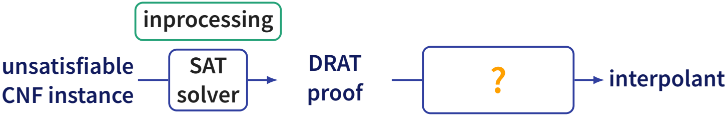


Inprocessing techniques and DRAT proofs

- Inprocessing techniques cannot be expressed by resolution proofs.

Interpolant generation

The good old times are gone

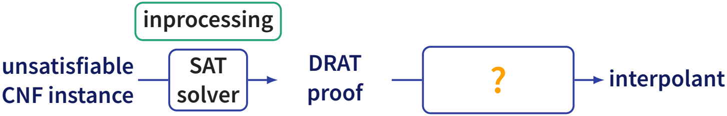


Inprocessing techniques and DRAT proofs

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

Interpolant generation

The good old times are gone

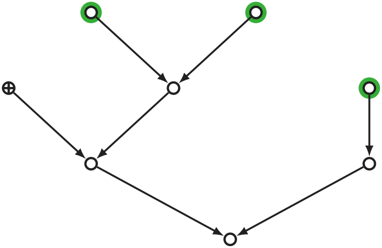


Inprocessing techniques and DRAT proofs

- 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.

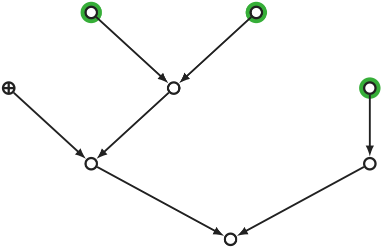
DRAT proofs

DRAT proofs



DRAT proofs

DRAT proofs



RAT,
not a consequence

DRAT proofs

DRAT proofs

RAT,
not a consequence

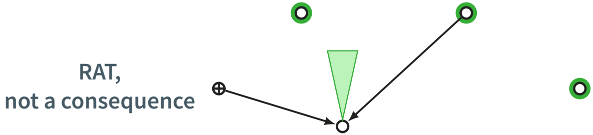
DRAT proofs

DRAT proofs

RAT,
not a consequence

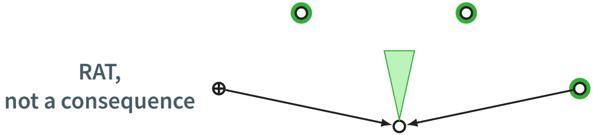
DRAT proofs

DRAT proofs



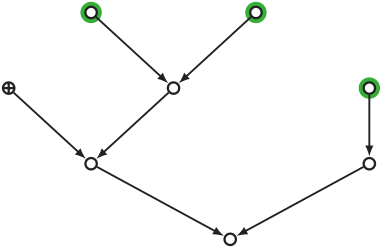
DRAT proofs

DRAT proofs



DRAT proofs

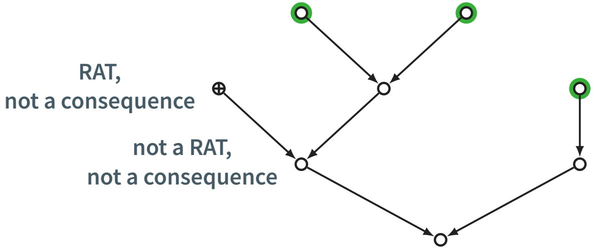
DRAT proofs



RAT,
not a consequence

DRAT proofs

DRAT proofs

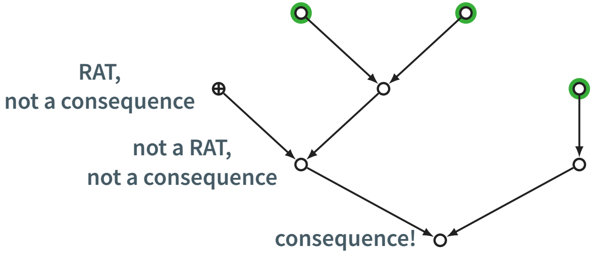


RAT,
not a consequence

not a RAT,
not a consequence

DRAT proofs

DRAT proofs



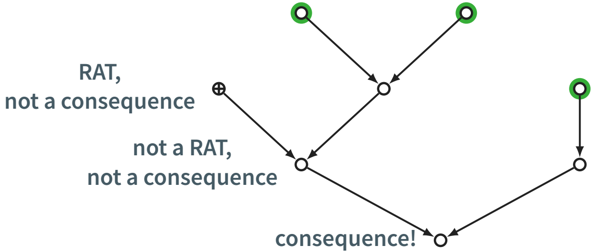
RAT,
not a consequence

not a RAT,
not a consequence

consequence!

DRAT proofs

DRAT proofs



RAT,
not a consequence

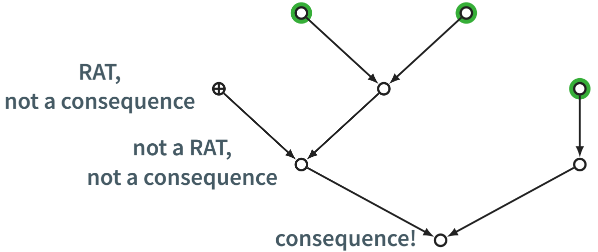
not a RAT,
not a consequence

consequence!

Some invariant seems to be preserved...

DRAT proofs

DRAT proofs

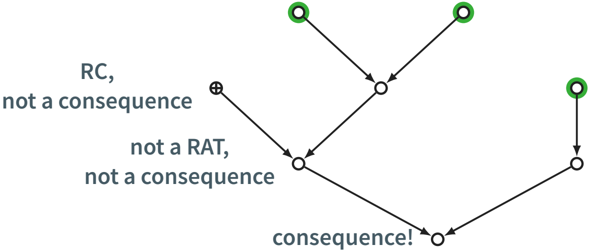


Some invariant seems to be preserved...

resolution consequence *[Philipp, Rebola-Pardo: LPAR '17]*

DRAT proofs

DRAT proofs



RC,
not a consequence

not a RAT,
not a consequence

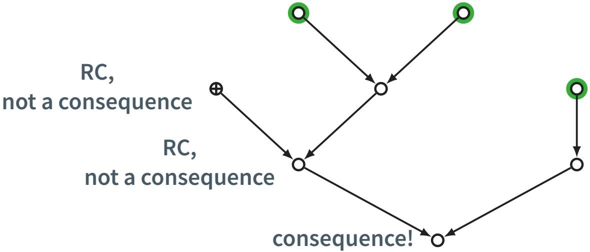
consequence!

Some invariant seems to be preserved…

resolution consequence *[Philipp, Rebola-Pardo: LPAR ’17]*

DRAT proofs

DRAT proofs

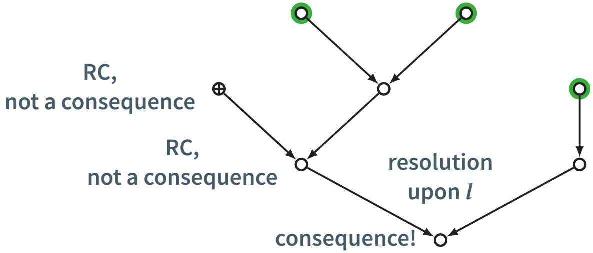


Some invariant seems to be preserved...

resolution consequence *[Philipp, Rebola-Pardo: LPAR ’17]*

DRAT proofs

DRAT proofs



RC,
not a consequence

RC,
not a consequence

resolution
upon l

consequence!

Some invariant seems to be preserved…

resolution consequence *[Philipp, Rebola-Pardo: LPAR ’17]*

Interpolation from DRAT proofs

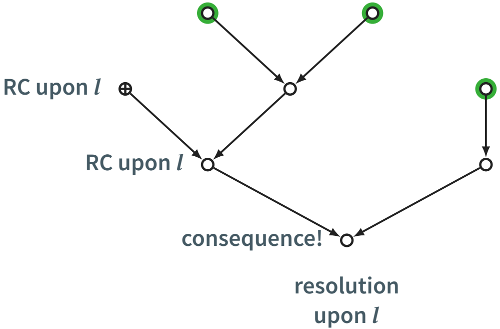
Idea convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

Interpolation from DRAT proofs

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

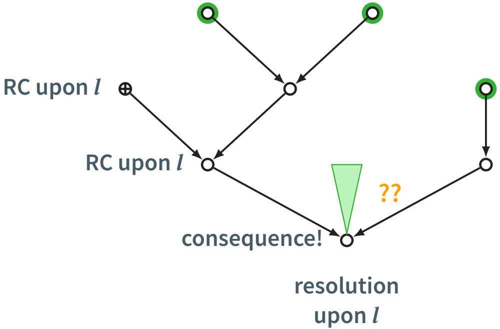
RAT elimination



Interpolation from DRAT proofs

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

RAT elimination

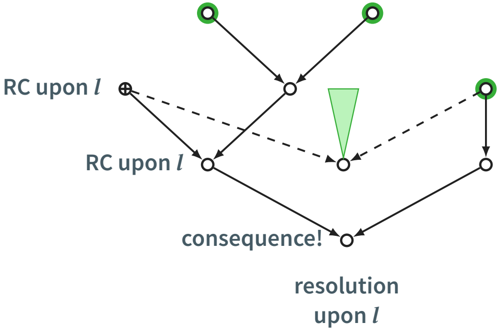


Interpolation from DRAT proofs

Idea convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

RAT elimination

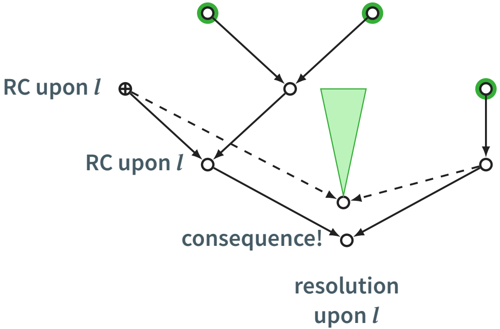


Interpolation from DRAT proofs

Idea convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

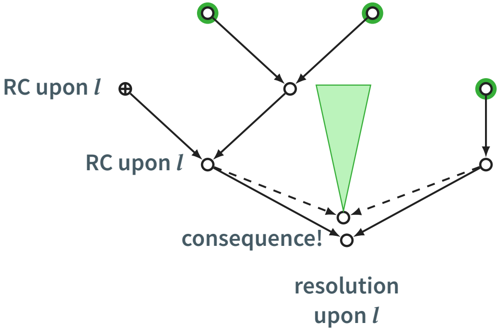
RAT elimination



Interpolation from DRAT proofs

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

RAT elimination

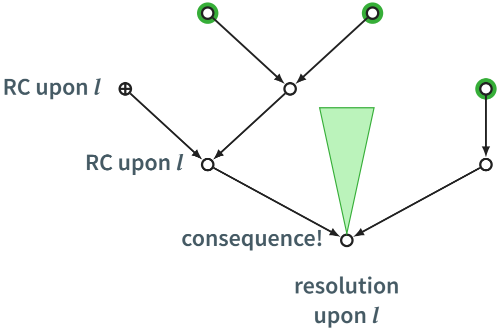


Interpolation from DRAT proofs

Idea convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

RAT elimination

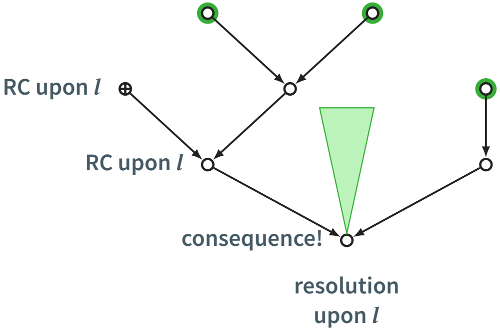


Interpolation from DRAT proofs

Idea convert DRAT proofs to resolution proofs

[Rebola-Pardo, Weissenbacher: manuscript]

RAT elimination

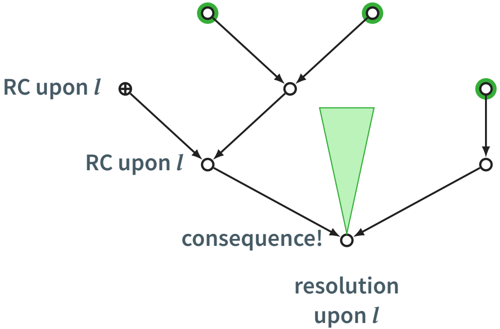


Good news an interpolant can be generated from a resolution proof

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...