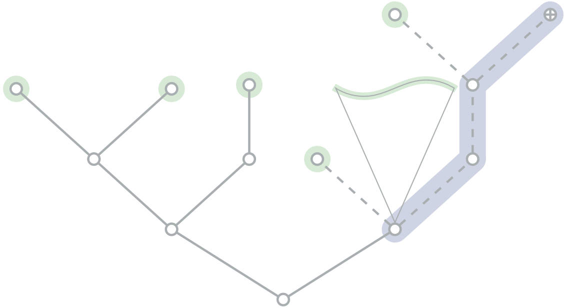
TECHNISCHE
UNIVERSITÄT
WIEN
Vienna University of Technology

Interpolants from SAT solving certificates

Adrián Rebola-Pardo

TU Wien

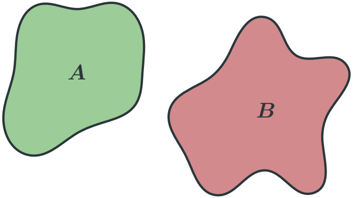


Automata, Logic and Games
Singapore

August 29th, 2016

Propositional interpolants

Let A, B be propositional formulae such that $A \wedge B$ is unsatisfiable.

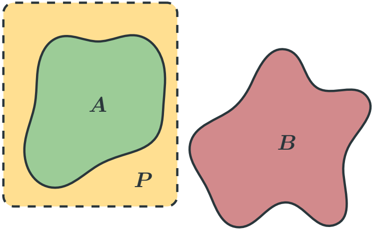


Propositional interpolants

Let A, B be propositional formulae such that $A \wedge B$ is unsatisfiable.

Interpolants an (A, B)-interpolant is a propositional formula P such that:

- $A \models P$.
- $P \wedge B$ is unsatisfiable.
- P contains only variables occurring in both A and B.

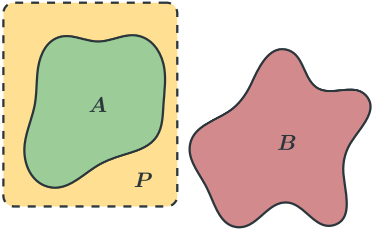


Propositional interpolants

Let A, B be propositional formulae such that $A \wedge B$ is unsatisfiable.

Interpolants an (A, B)-interpolant is a propositional formula P such that:

- $A \models P$.
- $P \wedge B$ is unsatisfiable.
- P contains only variables occurring in both A and B.



Interpolants are essential tools in formal methods and software verification:

- (Un)bounded model checking [McMillan '03]
- Boolean synthesis [Jiang et al. '09]
- Fault localization [Ermis et al. '12]
- Hardware verification [Keng Veneris '09]

Interpolation in practice

Interpolant generation

The good old times...

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

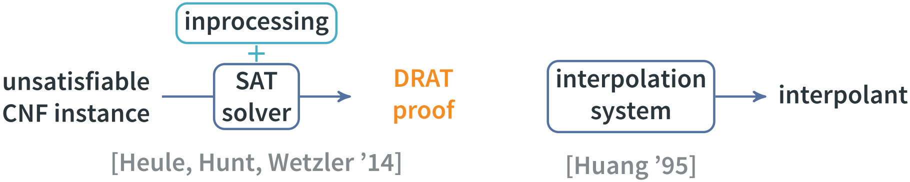
[Zhang, Malik ’03] [Huang ’95]

Interpolant generation

The good old times are gone

Interpolant generation

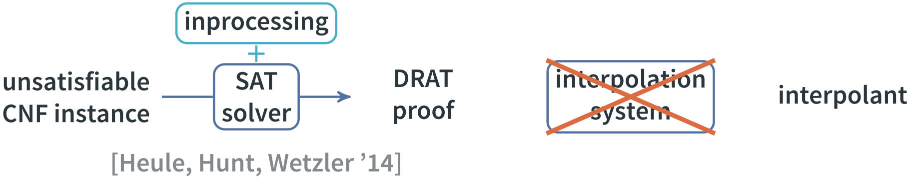
The good old times are gone



Properties of DRAT proofs

- ✔ Shorter and easier to generate or check than resolution proofs.
- ✔ Allow to express satisfiability-preserving techniques.

The good old times are gone



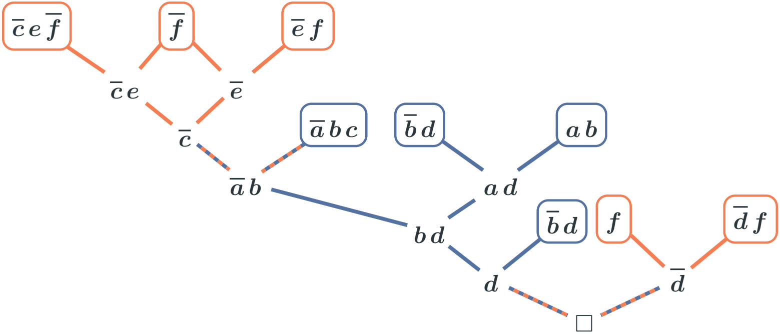
Properties of DRAT proofs

- ✔ Shorter and easier to generate or check than resolution proofs.
- ✔ Allow to express satisfiability-preserving techniques.
- ✘ We do not know how to generate interpolants from DRAT proofs.

Interpolants from resolution proofs

Example

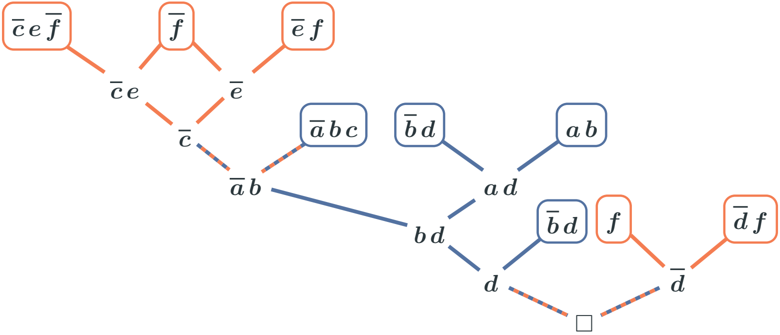
$$A = (\overline{a}\, b\, c) \wedge (\overline{b}\, d) \wedge (a\, b) \qquad B = (\overline{c}\, e\, \overline{f}) \wedge (\overline{e}\, f) \wedge (\overline{d}\, f) \wedge (\overline{f})$$



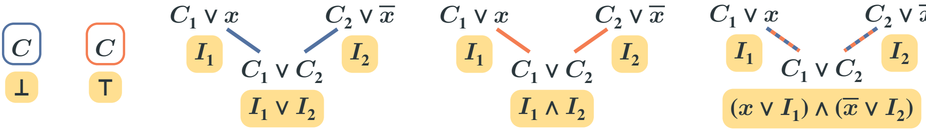
Interpolants from resolution proofs

Example

$A = (\overline{a}\,b\,c) \wedge (\overline{b}\,d) \wedge (a\,b)$ $\qquad B = (\overline{c}\,e\,\overline{f}) \wedge (\overline{e}\,f) \wedge (\overline{d}\,f) \wedge (\overline{f})$

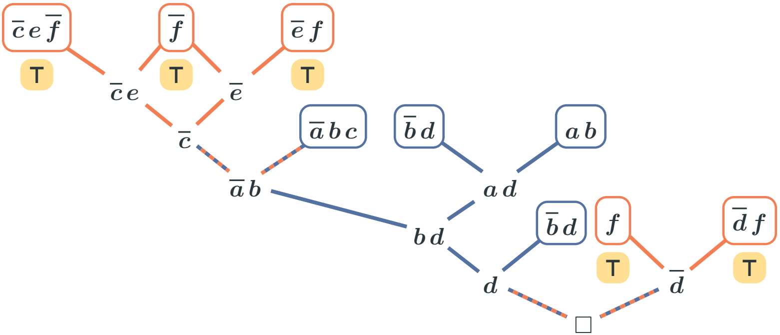


Interpolation rules [Huang '95]

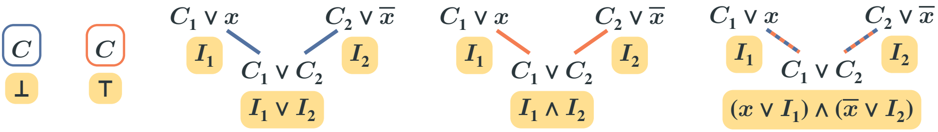


Example

$$A = (\overline{a}\, b\, c) \wedge (\overline{b}\, d) \wedge (a\, b) \qquad B = (\overline{c}\, e\, f) \wedge (\overline{e}\, f) \wedge (\overline{d}\, f) \wedge (\overline{f})$$



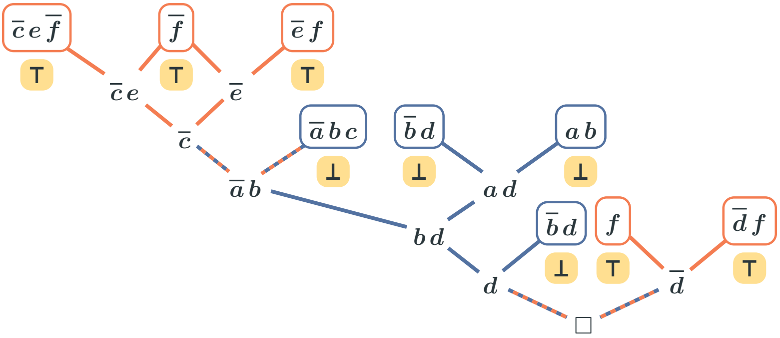
Interpolation rules [Huang '95]



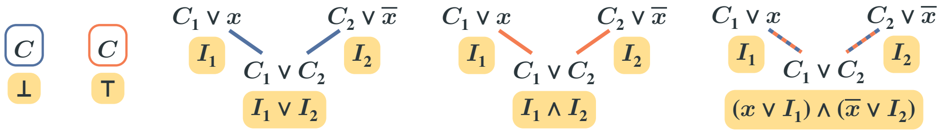
Interpolants from resolution proofs

Example

$$A = (\overline{a}\, b\, c) \land (\overline{b}\, d) \land (a\, b) \qquad B = (\overline{c}\, e\, \overline{f}) \land (\overline{e}\, f) \land (\overline{d}\, f) \land (\overline{f})$$



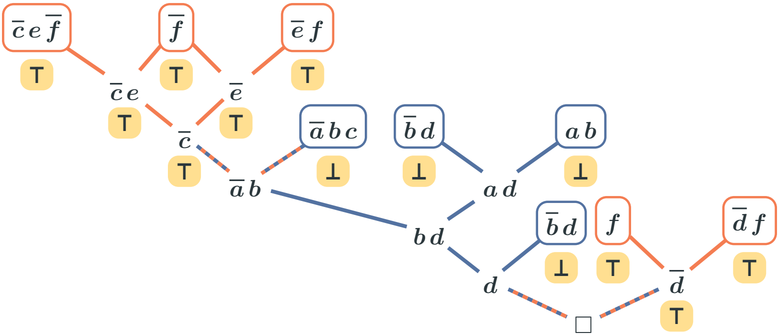
Interpolation rules [Huang ’95]



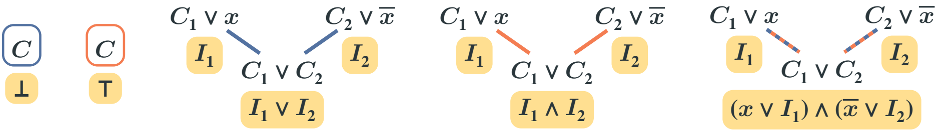
Interpolants from resolution proofs

Example

$A = (\overline{a}\, b\, c) \wedge (\overline{b}\, d) \wedge (a\, b) \qquad B = (\overline{c}\, e\, \overline{f}) \wedge (\overline{e}\, f) \wedge (\overline{d}\, f) \wedge (\overline{f})$

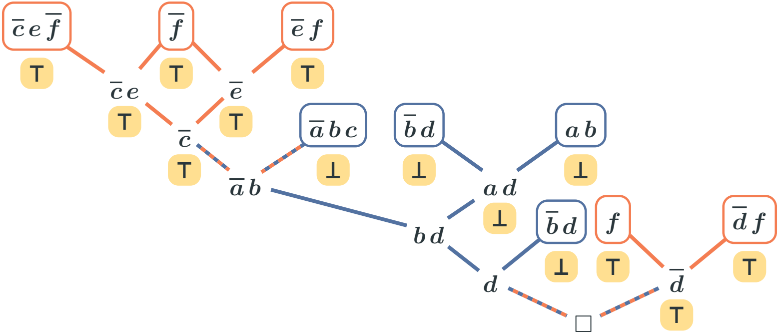


Interpolation rules [Huang '95]

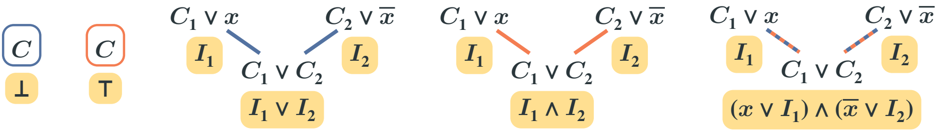


Example

$$A = (\overline{a}\, b\, c) \wedge (\overline{b}\, d) \wedge (a\, b) \qquad B = (\overline{c}\, e\, \overline{f}) \wedge (\overline{e}\, f) \wedge (\overline{d}\, f) \wedge (\overline{f})$$



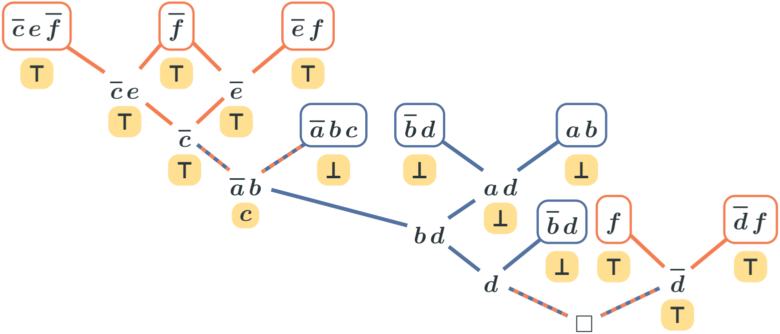
Interpolation rules [Huang '95]



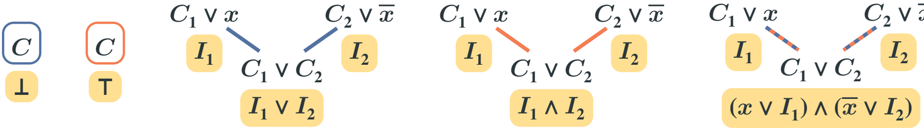
Interpolants from resolution proofs

Example

$$A = (\overline{a}\, b\, c) \wedge (\overline{b}\, d) \wedge (a\, b) \qquad B = (\overline{c}\, e\, f) \wedge (\overline{e}\, f) \wedge (\overline{d}\, f) \wedge (\overline{f})$$



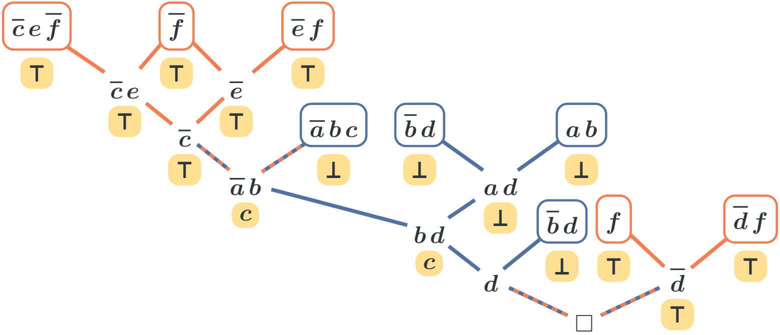
Interpolation rules [Huang '95]



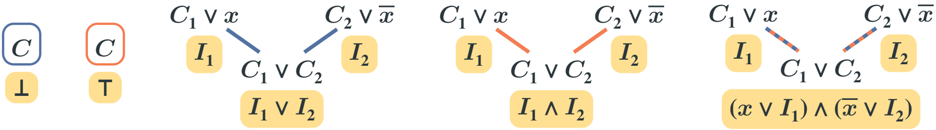
Interpolants from resolution proofs

Example

$$A = (\overline{a}\, b\, c) \wedge (\overline{b}\, d) \wedge (a\, b) \qquad B = (\overline{c}\, e\, \overline{f}) \wedge (\overline{e}\, f) \wedge (\overline{d}\, f) \wedge (\overline{f})$$



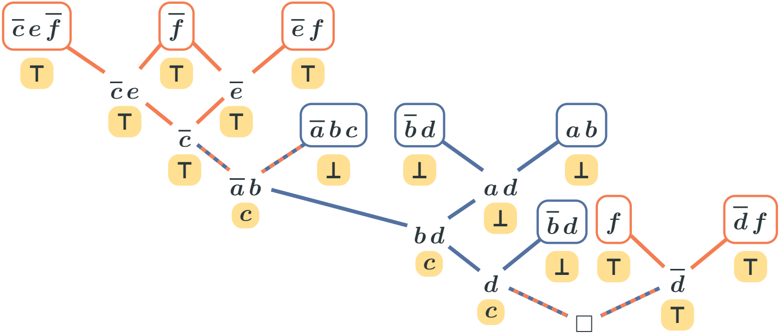
Interpolation rules [Huang ’95]



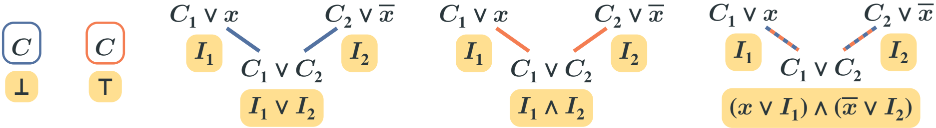
Interpolants from resolution proofs

Example

$$A = (\overline{a}\, b\, c) \wedge (\overline{b}\, d) \wedge (a\, b) \qquad B = (\overline{c}\, e\, \overline{f}) \wedge (\overline{e}\, f) \wedge (\overline{d}\, f) \wedge (\overline{f})$$



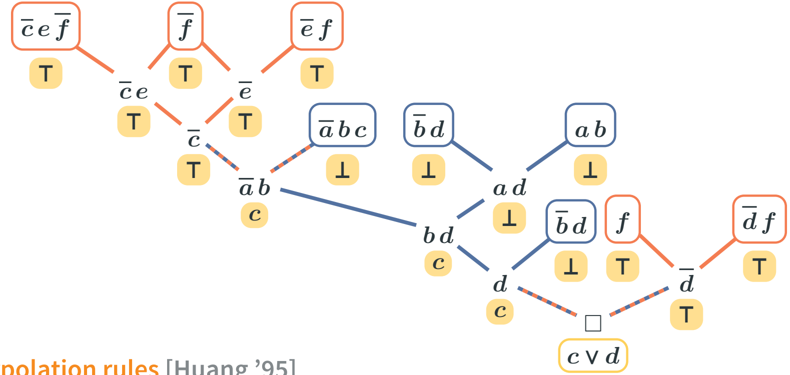
Interpolation rules [Huang ’95]



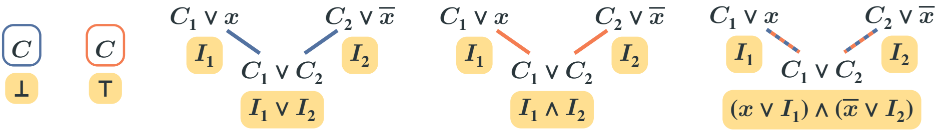
Interpolants from resolution proofs

Example

$A = (\overline{a}\, b\, c) \wedge (\overline{b}\, d) \wedge (a\, b) \qquad B = (\overline{c}\, e\, \overline{f}) \wedge (\overline{e}\, f) \wedge (\overline{d}\, f) \wedge (\overline{f})$

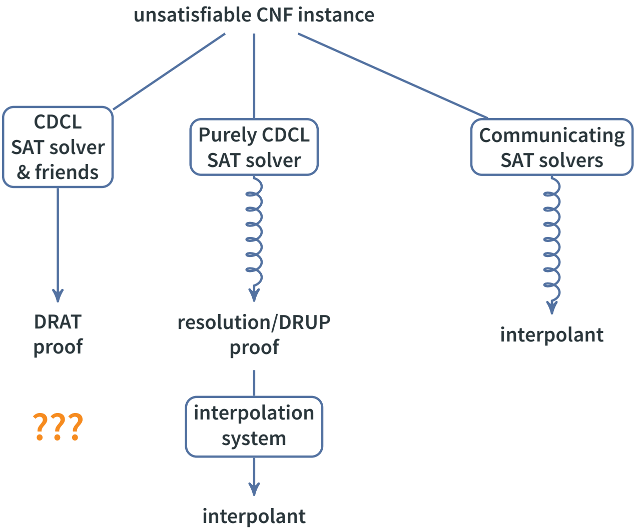


Interpolation rules [Huang ’95]

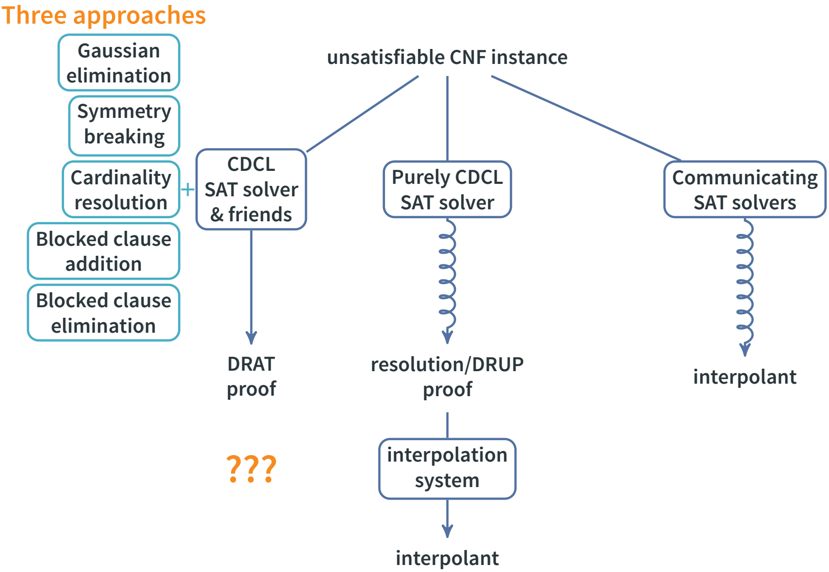


Interpolant generation from proofs

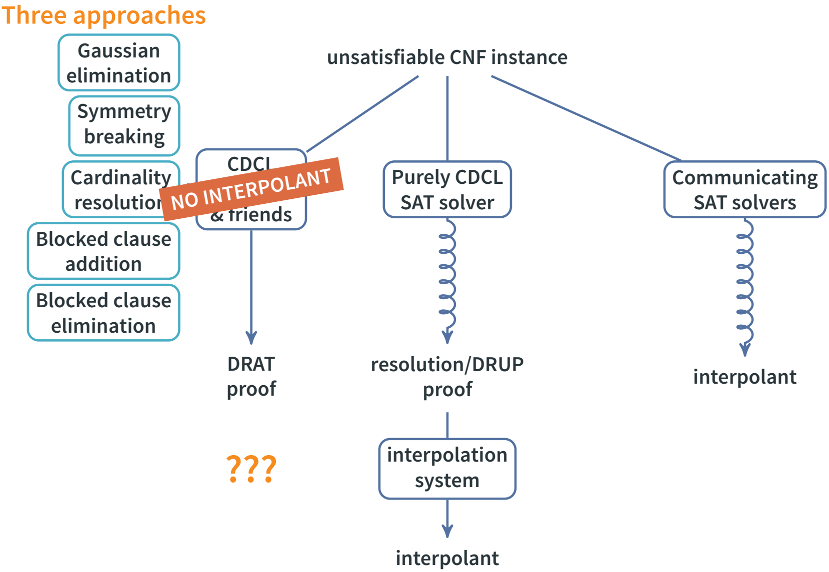
Three approaches



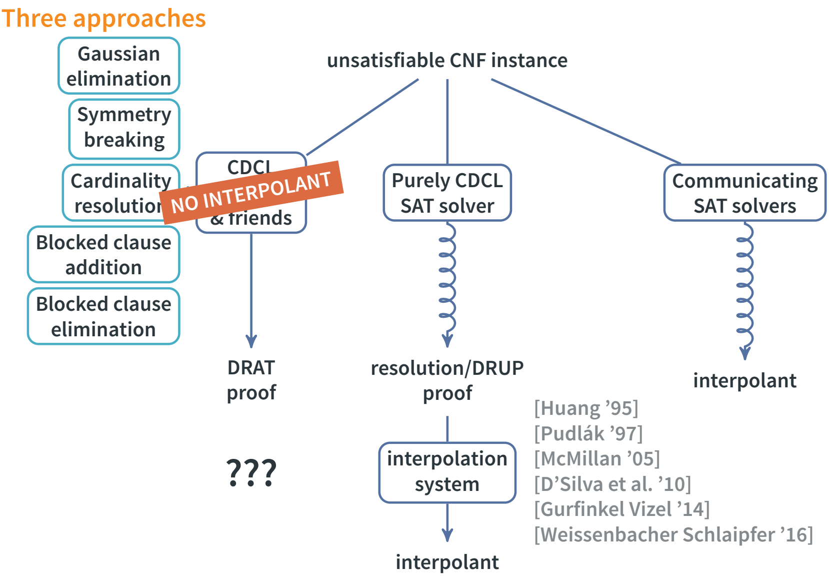
Interpolant generation from proofs



Interpolant generation from proofs

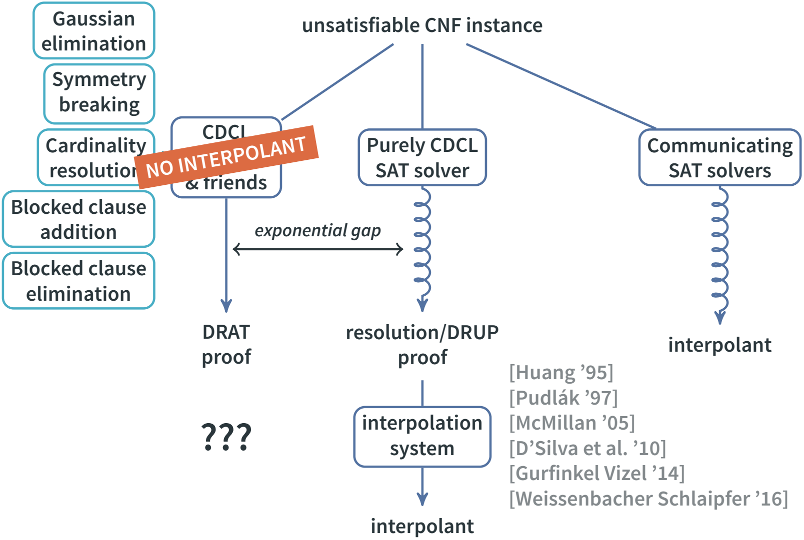


Interpolant generation from proofs



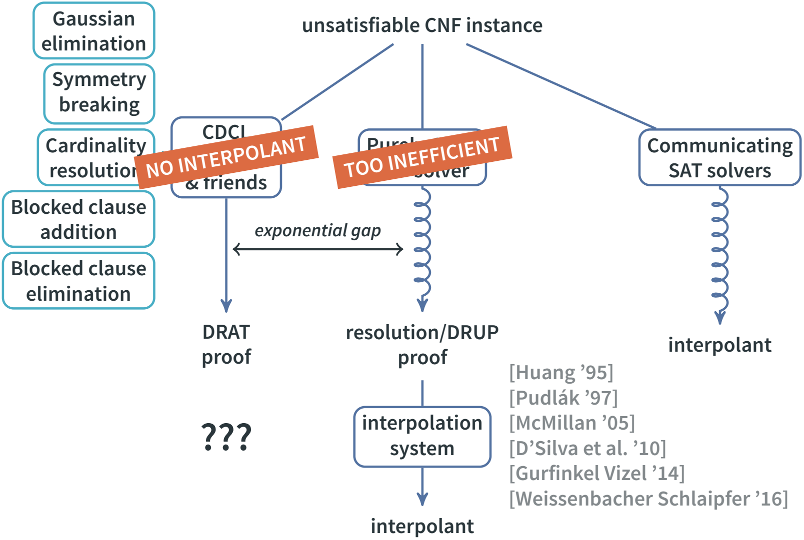
Interpolant generation from proofs

Three approaches



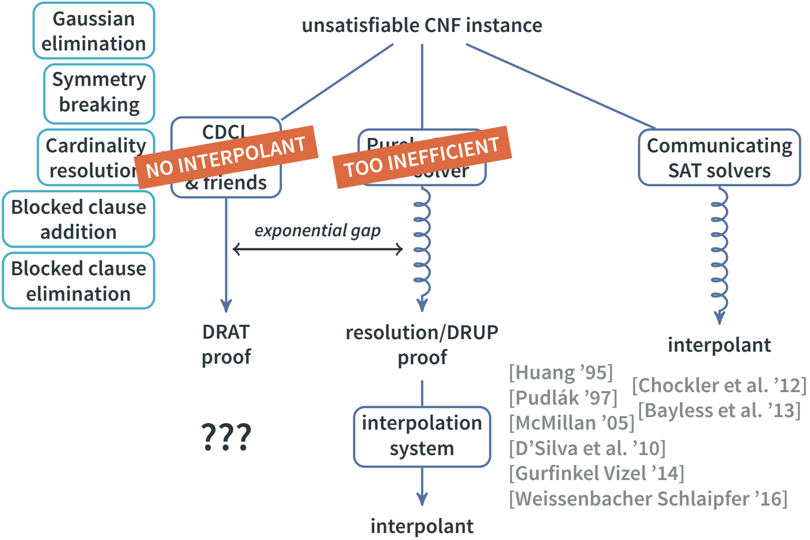
Interpolant generation from proofs

Three approaches



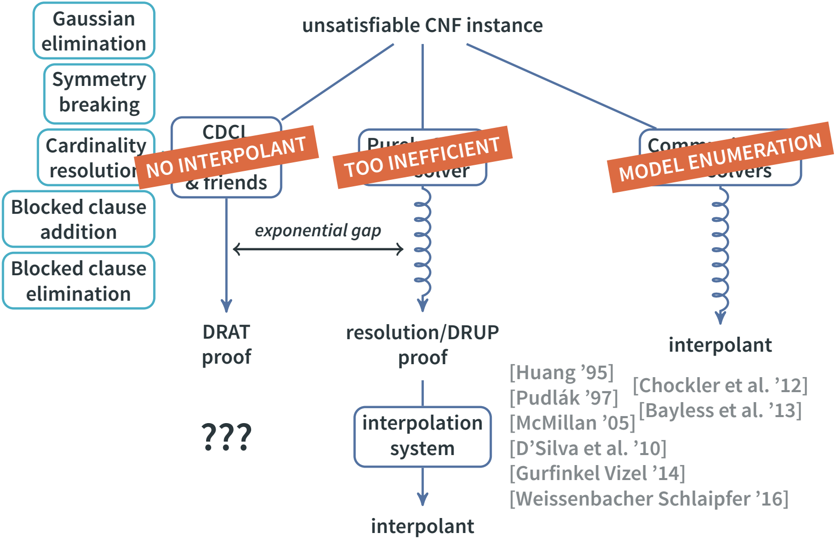
Interpolant generation from proofs

Three approaches

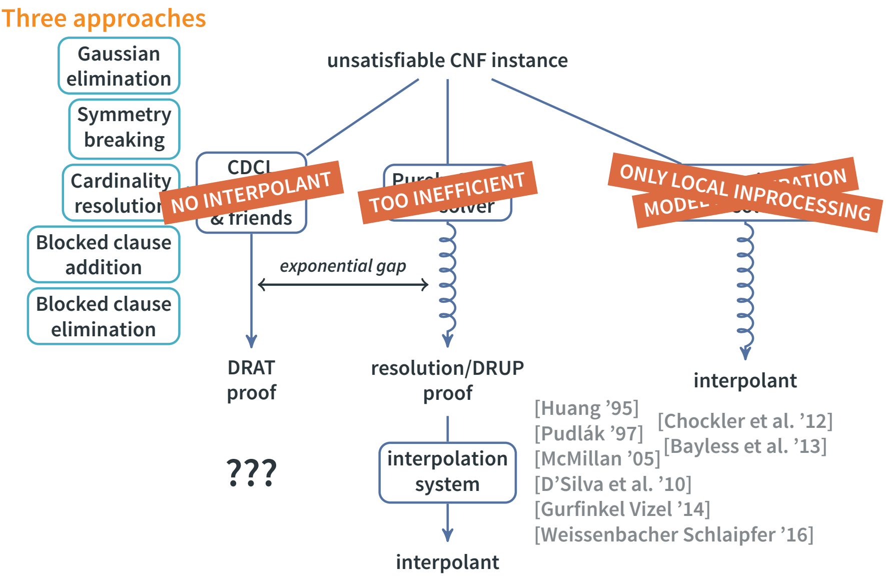


Interpolant generation from proofs

Three approaches

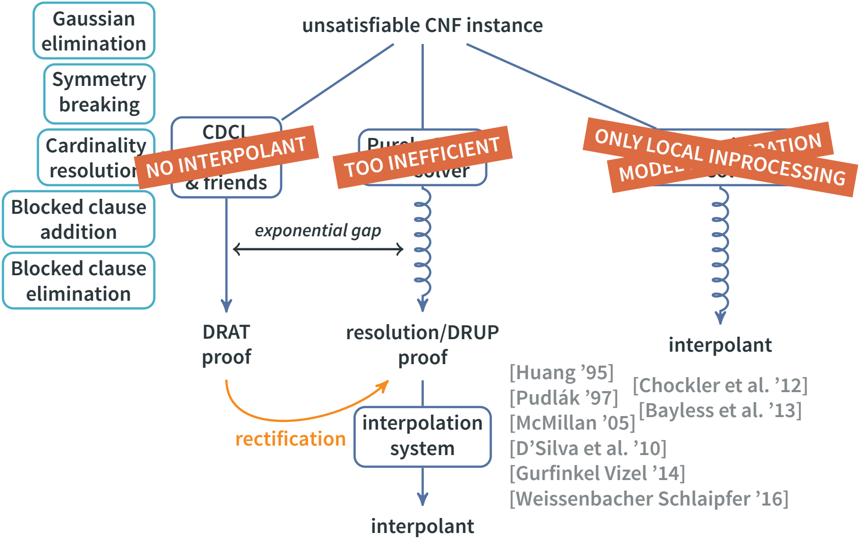


Interpolant generation from proofs



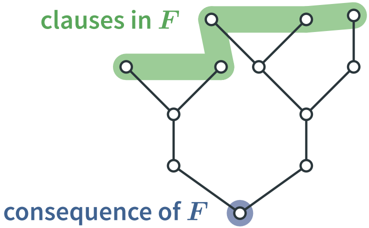
Interpolant generation from proofs

Three approaches



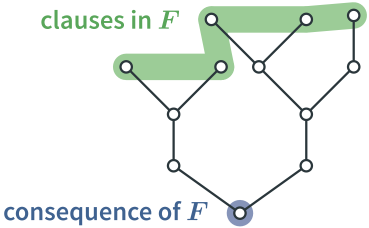
Proof systems for SAT solvers

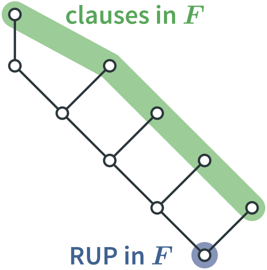
Reverse Unit Propagation (RUP)



DRUP proofs

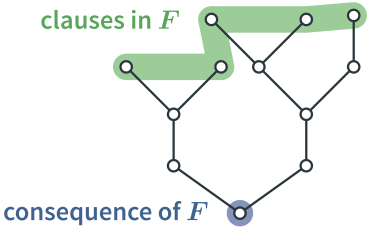
Reverse Unit Propagation (RUP)

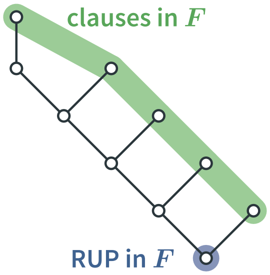




DRUP proofs

Reverse Unit Propagation (RUP)

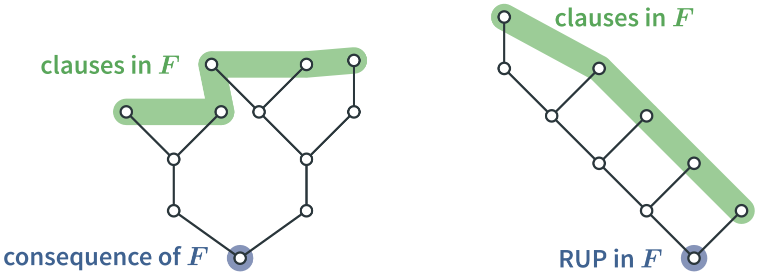




DRUP proof system RUP introduction + arbitrary clause deletion

DRUP proofs

Reverse Unit Propagation (RUP)



DRUP proof system RUP introduction + arbitrary clause deletion

- Essentially as powerful as resolution [Beame et al. ’04]
- Interpolants can be easily generated [Gurfinkel Vizel ’14]

Resolution asymmetric tautologies

A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.

Resolution asymmetric tautologies

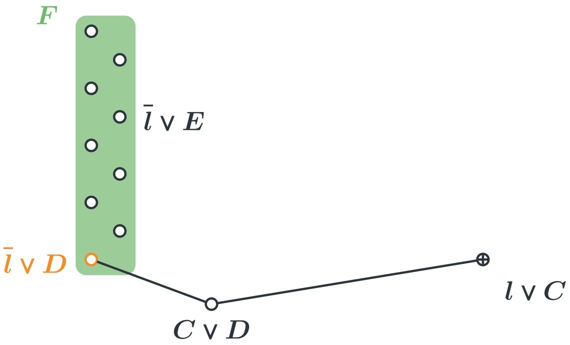
A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.

Resolution asymmetric tautologies

A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.

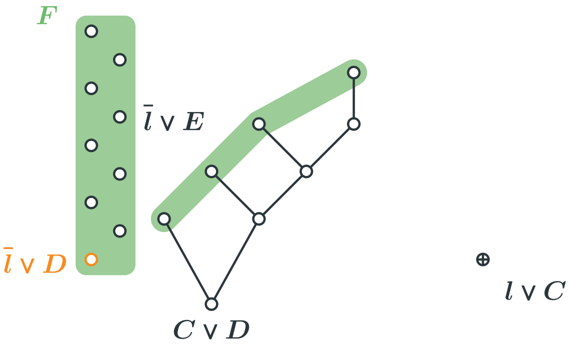
Resolution asymmetric tautologies

A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.



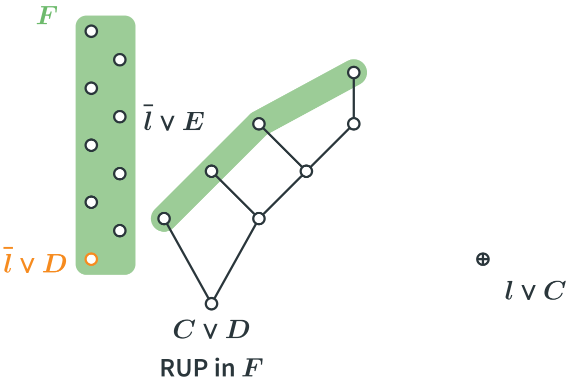
Resolution asymmetric tautologies

A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.



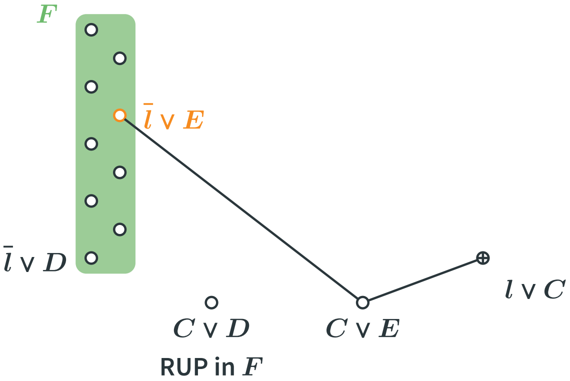
Resolution asymmetric tautologies

A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.



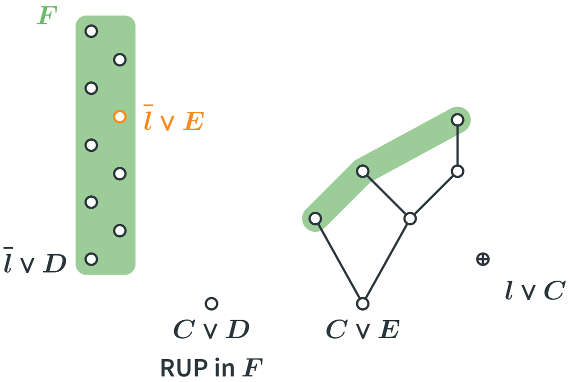
Resolution asymmetric tautologies

A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.



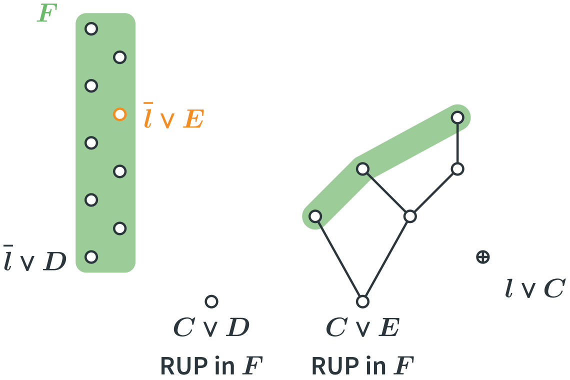
Resolution asymmetric tautologies

A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.



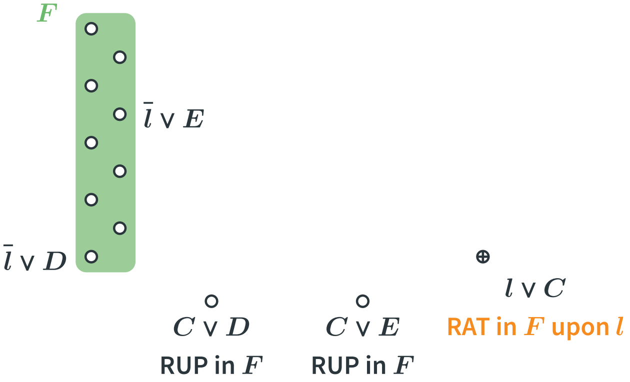
Resolution asymmetric tautologies

A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.



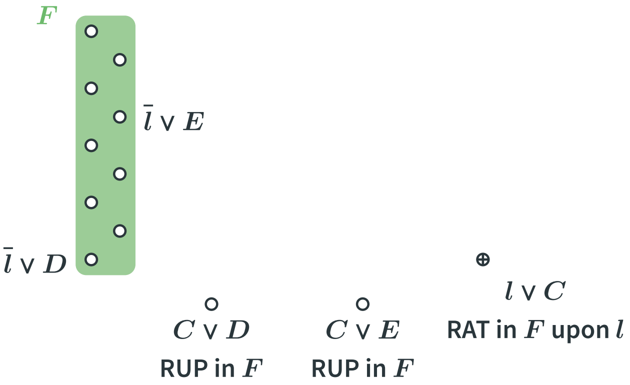
Resolution asymmetric tautologies

A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.



Resolution asymmetric tautologies

A clause C is a resolution asymmetric tautology (RAT) in a CNF formula F upon a literal l if every resolvent $C \otimes D$ upon l, where $D \in F$, is a RUP in F.



Theorem If C is a RAT in F, then F is satisfiable if and only if $F \cup \{C\}$ is.

RAT introduction can be used as an inference rule of a proof system.

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

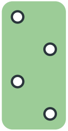
Extended resolution can be simulated by DRAT

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



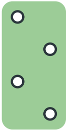
$$p \leftrightarrow q \wedge r \quad \equiv \quad (\neg p \vee q) \;\wedge\; (\neg p \vee r) \;\wedge\; (p \vee \neg q \vee \neg r)$$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



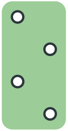
DRAT proof $(\neg p \vee q)^{\text{RAT}}$, $(\neg p \vee r)^{\text{RAT}}$, $(p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



○ $\neg p \vee q$

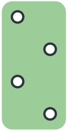
DRAT proof $(\neg p \vee q)^{\mathsf{RAT}}$, $(\neg p \vee r)^{\mathsf{RAT}}$, $(p \vee \neg q \vee \neg r)^{\mathsf{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



no resolvents

○ $\neg p \vee q$

RAT upon $\neg p$

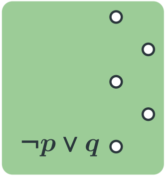
DRAT proof $(\neg p \vee q)^{\text{RAT}}$, $(\neg p \vee r)^{\text{RAT}}$, $(p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



DRAT proof $(\neg p \vee q)^{\text{RAT}}, (\neg p \vee r)^{\text{RAT}}, (p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT

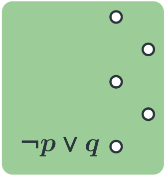
DRAT proof $(\neg p \vee q)^{\text{RAT}}$, $(\neg p \vee r)^{\text{RAT}}$, $(p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



no resolvents

$\neg p \vee r$

RAT upon $\neg p$

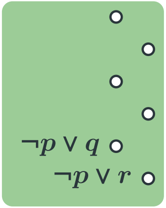
DRAT proof $(\neg p \vee q)^{\mathsf{RAT}}$, $(\neg p \vee r)^{\mathsf{RAT}}$, $(p \vee \neg q \vee \neg r)^{\mathsf{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



DRAT proof $(\neg p \vee q)^{\text{RAT}}$, $(\neg p \vee r)^{\text{RAT}}$, $(p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT

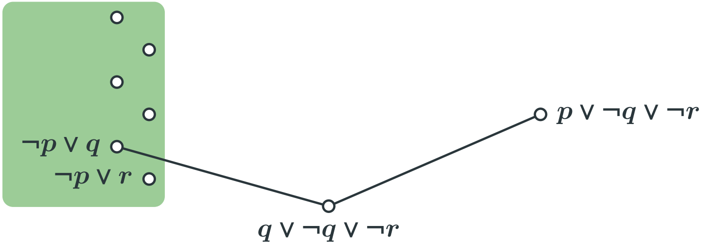
DRAT proof $(\neg p \vee q)^{\text{RAT}}, (\neg p \vee r)^{\text{RAT}}, (p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



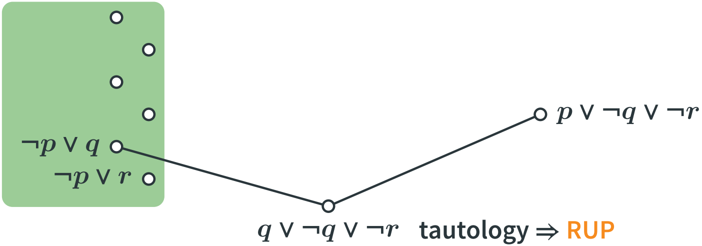
DRAT proof $(\neg p \vee q)^{\text{RAT}}$, $(\neg p \vee r)^{\text{RAT}}$, $(p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



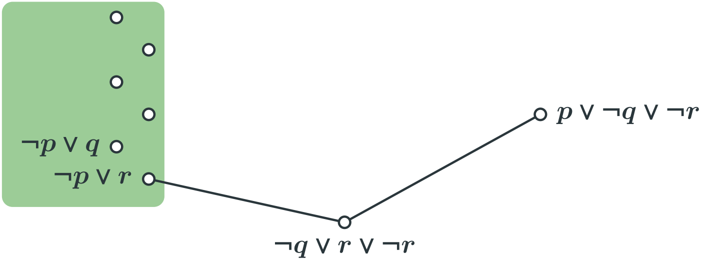
DRAT proof $(\neg p \vee q)^{\text{RAT}}, (\neg p \vee r)^{\text{RAT}}, (p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



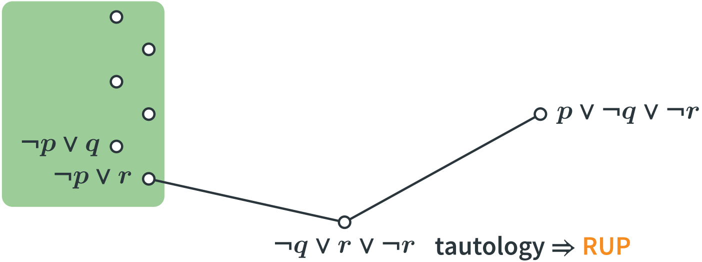
DRAT proof $(\neg p \vee q)^{\mathsf{RAT}}, (\neg p \vee r)^{\mathsf{RAT}}, (p \vee \neg q \vee \neg r)^{\mathsf{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT



DRAT proof $(\neg p \vee q)^{\text{RAT}}, (\neg p \vee r)^{\text{RAT}}, (p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT

$\neg p \vee q$

$\neg p \vee r$

$p \vee \neg q \vee \neg r$

RAT upon p

DRAT proof $(\neg p \vee q)^{\text{RAT}}, (\neg p \vee r)^{\text{RAT}}, (p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT

$\neg p \vee q$

$\neg p \vee r$

$p \vee \neg q \vee \neg r$

DRAT proof $(\neg p \vee q)^{\text{RAT}}$, $(\neg p \vee r)^{\text{RAT}}$, $(p \vee \neg q \vee \neg r)^{\text{RAT}}$

The DRAT proof system

DRAT proof system RUP introduction + RAT introduction + arbitrary clause deletion

Extended resolution resolution + definitions $p \leftrightarrow q \wedge r$ where p is fresh

Extended resolution can be simulated by DRAT

$$\neg p \vee q$$
$$\neg p \vee r$$
$$p \vee \neg q \vee \neg r$$

Properties of extended resolution

- No lower bound for length of extended resolution proofs is known.
- Used to express inprocessing techniques used in SAT solvers.
- Lacks the efficient interpolation property.
- No interpolation method is known.

Partial soundness of DRAT

Partial soundness $F \vdash G \quad \not\Rightarrow \quad F \models G$

Partial soundness of DRAT

Partial soundness $F \vdash G \quad \not\Rightarrow \quad F \vDash G$

- A CNF formula is unsatisfiable iff there is a DRAT refutation.

Partial soundness of DRAT

Partial soundness $F \vdash G \quad \not\Rightarrow \quad F \vDash G$

- A CNF formula is unsatisfiable iff there is a DRAT refutation.
- Intermediate clauses are not necessarily consequences of the premise formula.

If p is fresh, then $F \nvDash F \wedge (p \leftrightarrow q \wedge r)$

Partial soundness of DRAT

Partial soundness $F \vdash G \quad \not\Rightarrow \quad F \vDash G$

- A CNF formula is unsatisfiable iff there is a DRAT refutation.
- Intermediate clauses are not necessarily consequences of the premise formula.

$$\text{If } p \text{ is fresh, then } F \not\vDash F \wedge (p \leftrightarrow q \wedge r)$$

- In fact, we can always derive any satisfiable CNF formula!

$$F = p \qquad (p)^{\text{DEL}},\ (\neg p)^{\text{RAT}} \qquad F' = \neg p$$

Partial soundness of DRAT

Partial soundness $F \vdash G \quad \not\Rightarrow \quad F \vDash G$

- A CNF formula is unsatisfiable iff there is a DRAT refutation.
- Intermediate clauses are not necessarily consequences of the premise formula.

If p is fresh, then $F \not\vDash F \wedge (p \leftrightarrow q \wedge r)$

- In fact, we can always derive any satisfiable CNF formula!

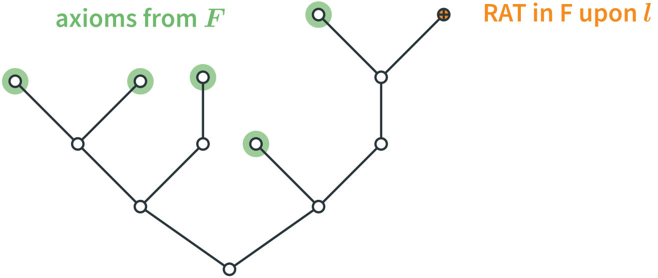
$$F = p \qquad (p)^{\mathsf{DEL}}, (\neg p)^{\mathsf{RAT}} \qquad F' = \neg p$$

Interpolation and soundness

- Interpolation algorithms work because an induction invariant holds for partial interpolants.
- This invariant strongly requires soundness of the proof system.

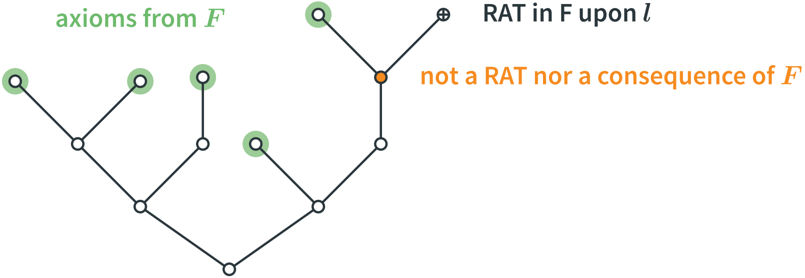
Interpolation from DRAT proofs

RATs, consequences and bindings



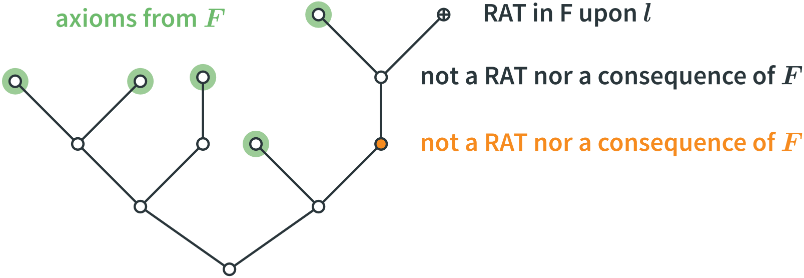
Why does RAT work? Eventually, some successor of every RAT becomes a consequence.

RATs, consequences and bindings



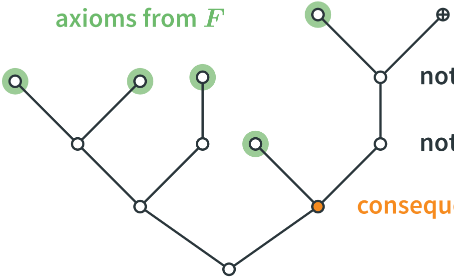
Why does RAT work? **Eventually, some successor of every RAT becomes a consequence.**

RATs, consequences and bindings



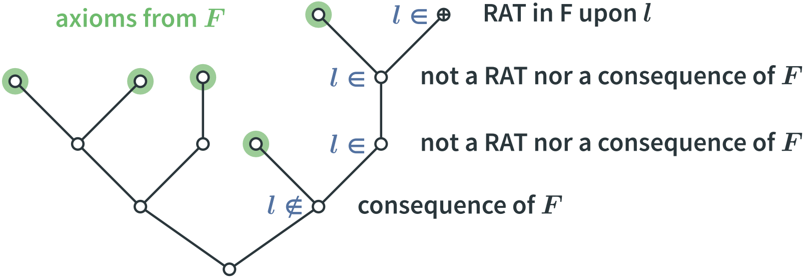
Why does RAT work? **Eventually, some successor of every RAT becomes a consequence.**

RATs, consequences and bindings



Why does RAT work? **Eventually, some successor of every RAT becomes a consequence.**

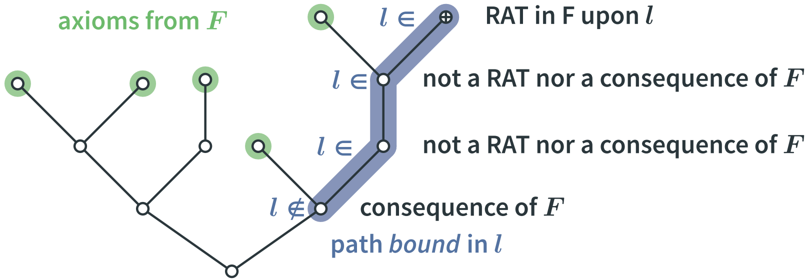
RATs, consequences and bindings



Why does RAT work? **Eventually, some successor of every RAT becomes a consequence.**

But *when*? **As soon as the pivot literal is eliminated by resolution.**

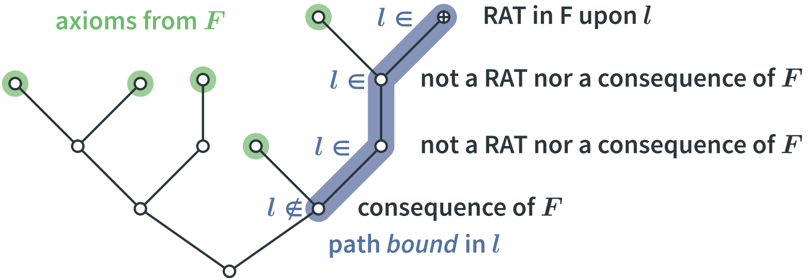
RATs, consequences and bindings



Why does RAT work? **Eventually, some successor of every RAT becomes a consequence.**

But *when*? **As soon as the pivot literal is eliminated by resolution.**

RATs, consequences and bindings



Why does RAT work? Eventually, some successor of every RAT becomes a consequence.

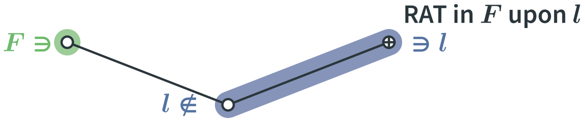
But *when*? As soon as the pivot literal is eliminated by resolution.

Question Can we obtain a resolution proof of that consequence clause?

Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving the RAT with a clause from F

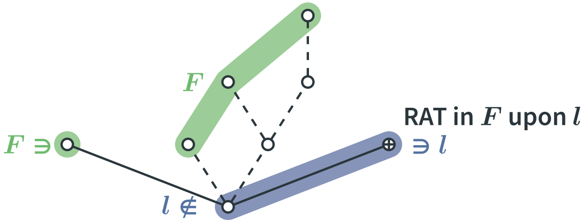


Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving the RAT with a clause from F

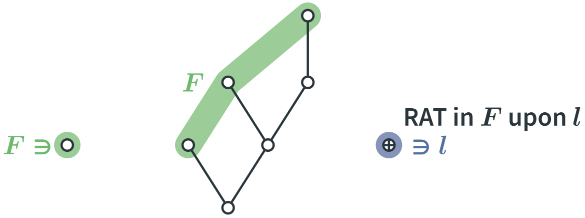
A proof can be extracted when checking the RAT property.



Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving the RAT with a clause from F

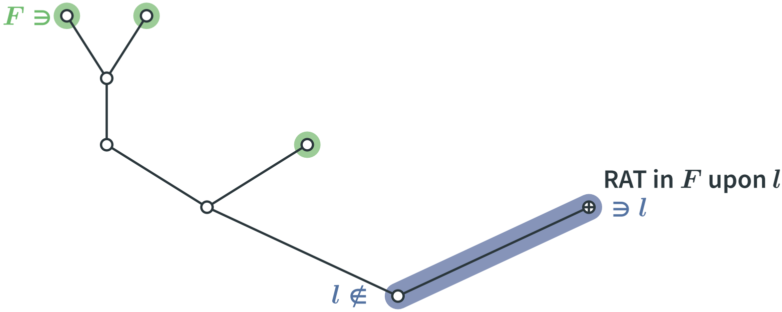
A proof can be extracted when checking the RAT property.



Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving the RAT with a consequence of F

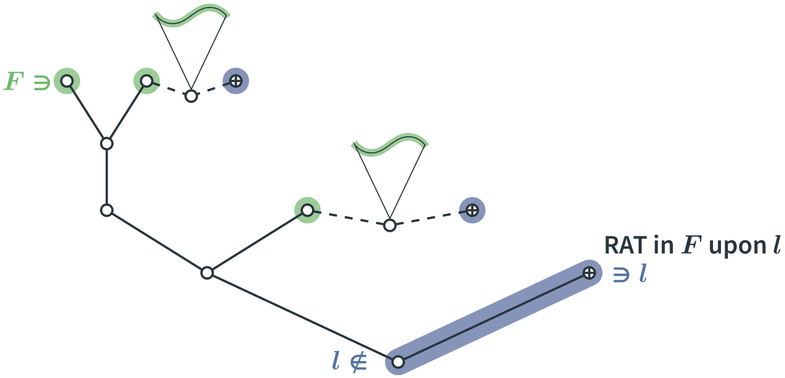


Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving the RAT with a consequence of F

Transform the RAT witnesses along the derivation of the consequence.

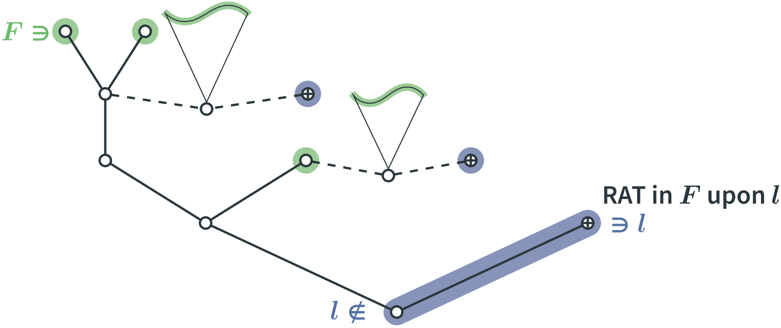


Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving the RAT with a consequence of F

Transform the RAT witnesses along the derivation of the consequence.

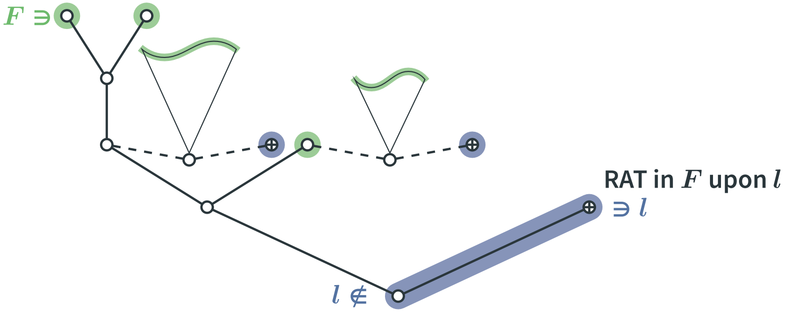


Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving the RAT with a consequence of F

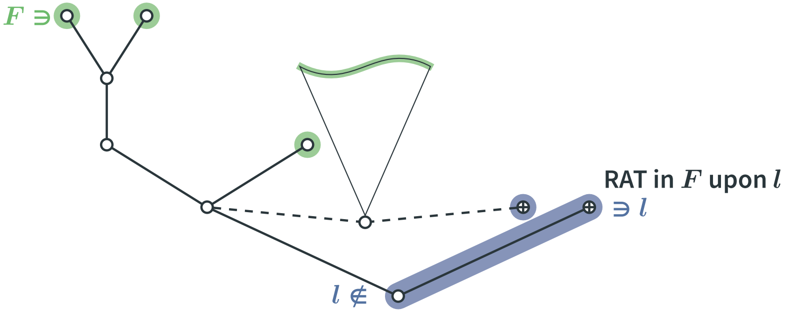
Transform the RAT witnesses along the derivation of the consequence.



Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving the RAT with a consequence of F

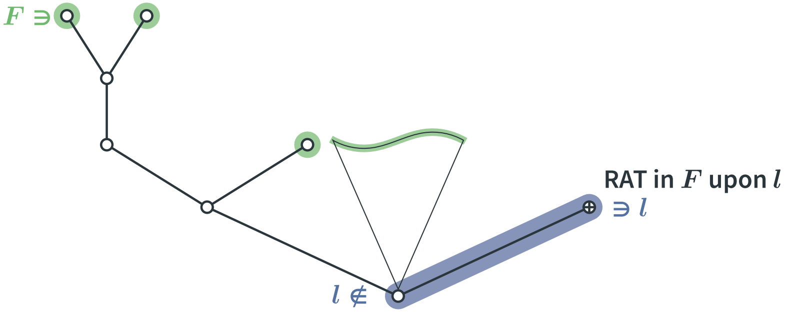
Transform the RAT witnesses along the derivation of the consequence.



Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving the RAT with a consequence of F
Transform the RAT witnesses along the derivation of the consequence.

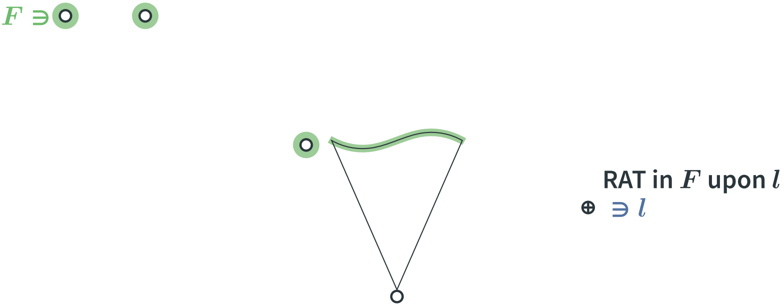


Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving the RAT with a consequence of F

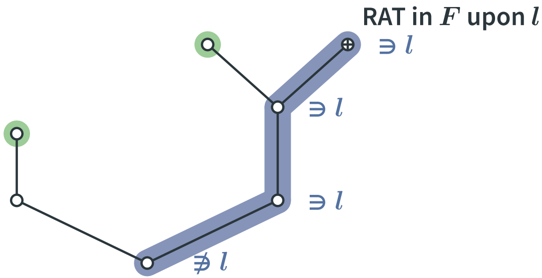
Transform the RAT witnesses along the derivation of the consequence.



Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving a consequence of the RAT with a consequence of F

Transform the RAT witnesses along the bound subproof.

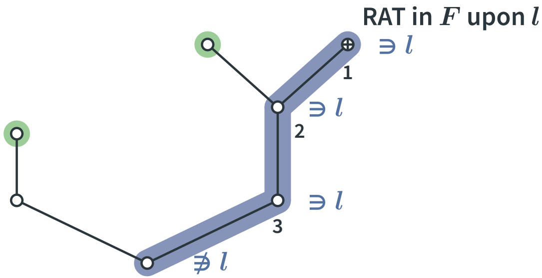


Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving a consequence of the RAT with a consequence of F

Transform the RAT witnesses along the bound subproof.

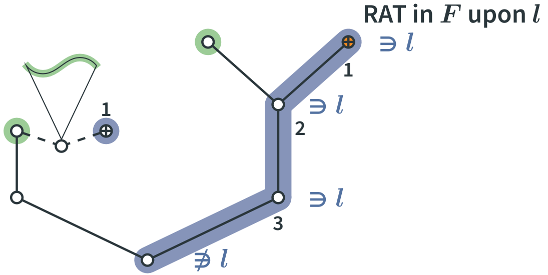


Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving a consequence of the RAT with a consequence of F

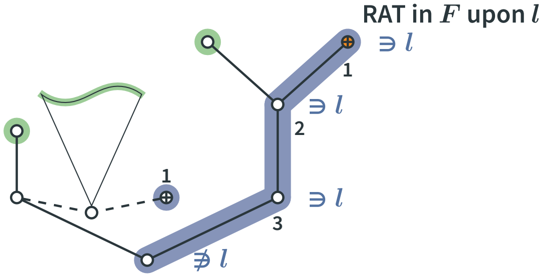
Transform the RAT witnesses along the bound subproof.



Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving a consequence of the RAT with a consequence of F

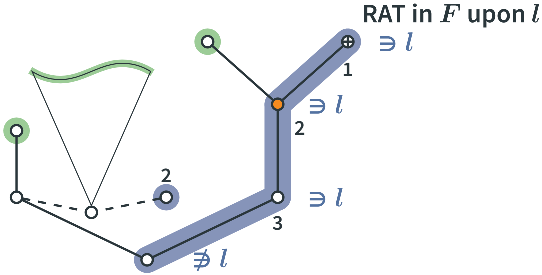
Transform the RAT witnesses along the bound subproof.



Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving a consequence of the RAT with a consequence of F

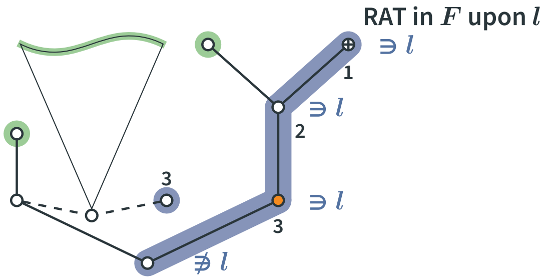
Transform the RAT witnesses along the bound subproof.



Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving a consequence of the RAT with a consequence of F

Transform the RAT witnesses along the bound subproof.

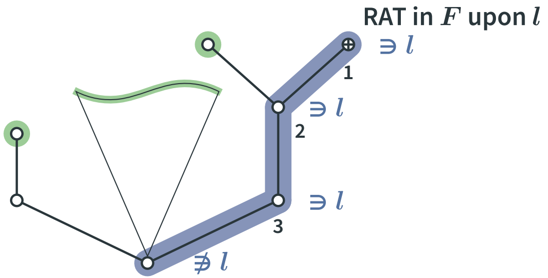


Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving a consequence of the RAT with a consequence of F

Transform the RAT witnesses along the bound subproof.

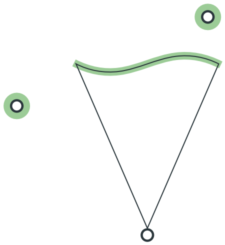


Refactoring DRAT proofs into resolution proofs

Question Can we obtain a resolution proof of that consequence clause?

Elimination by resolving a consequence of the RAT with a consequence of F

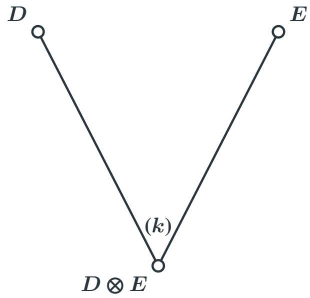
Transform the RAT witnesses along the bound subproof.



A closer look into rectification

C RAT upon F in l

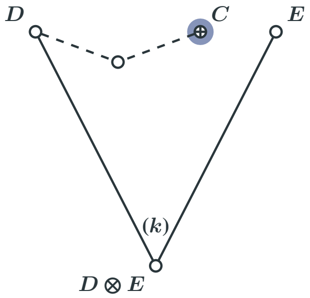
D, E clauses mutually resolvable upon k.



A closer look into rectification

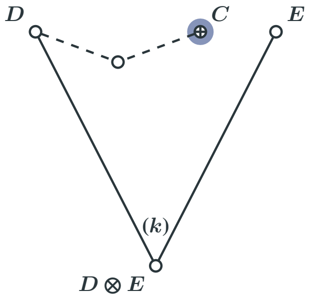
C RAT upon F in l
D, E clauses mutually resolvable upon k.

D is resolvable
with C upon l



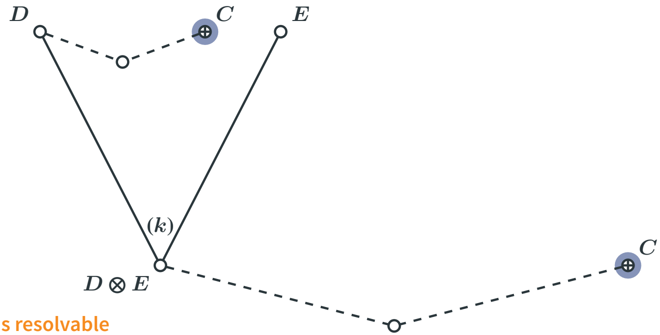
C	RAT upon F in l
D, E	clauses mutually resolvable upon k.

E is not resolvable
with C upon l



A closer look into rectification

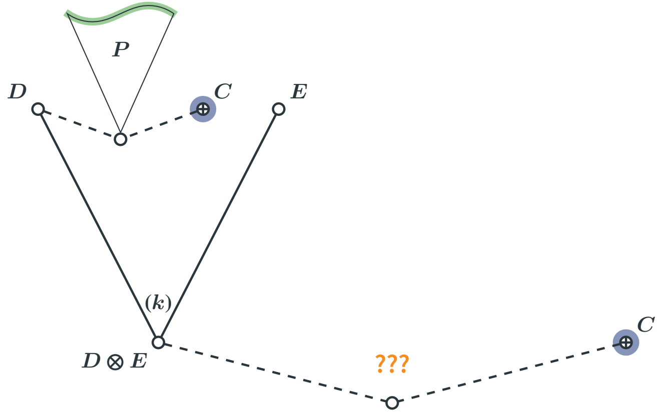
C RAT upon F in l
D, E clauses mutually resolvable upon k.



$D \otimes E$ is resolvable
with C upon l

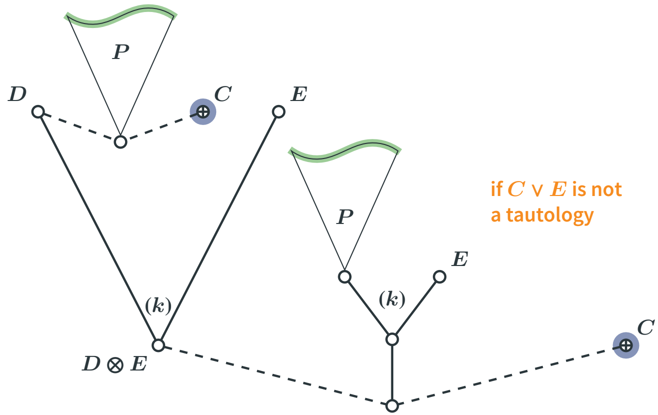
A closer look into rectification

C	RAT upon F in l
D, E	clauses mutually resolvable upon k.



A closer look into rectification

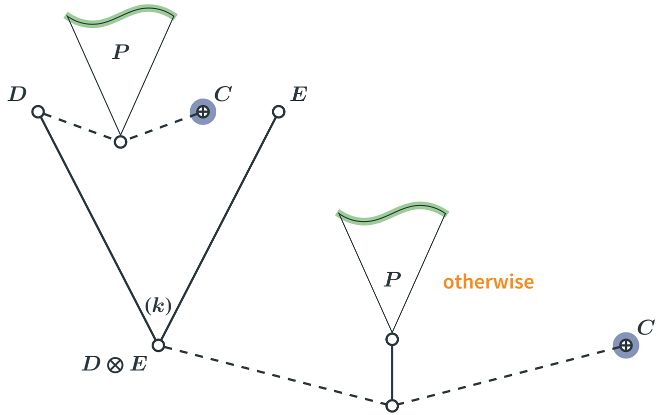
C	RAT upon F in l
D, E	clauses mutually resolvable upon k.



if $C \vee E$ is not
a tautology

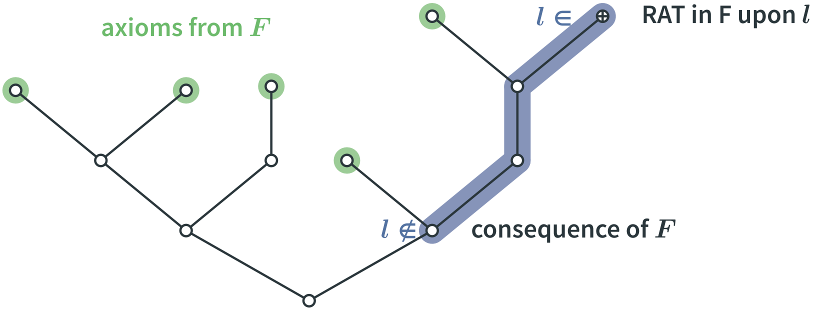
A closer look into rectification

C	RAT upon F in l
D, E	clauses mutually resolvable upon k.

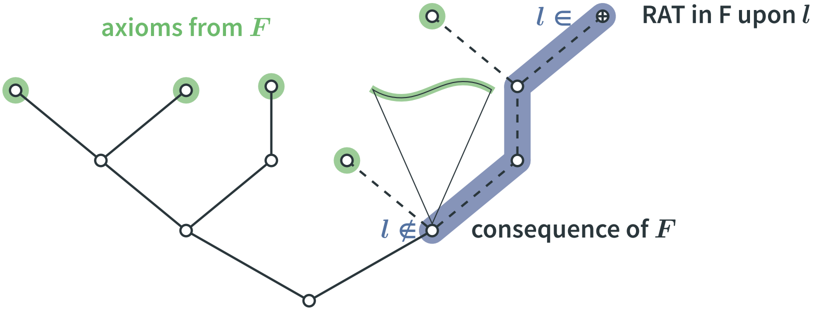


Interpolant generation from DRAT proofs

Interpolation by rectification into a resolution proof

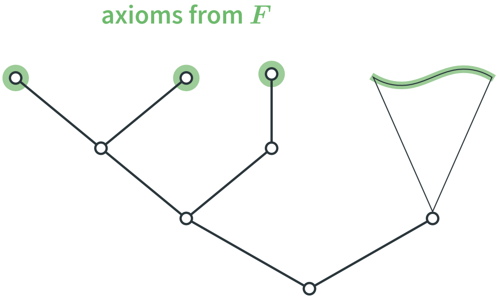


Interpolation by rectification into a resolution proof

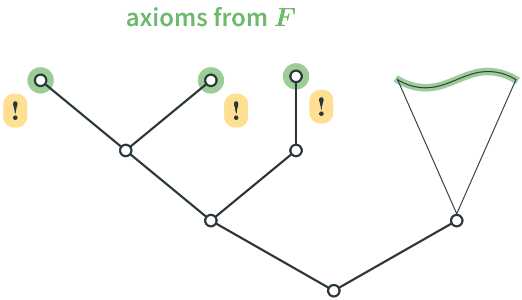


Interpolant generation from DRAT proofs

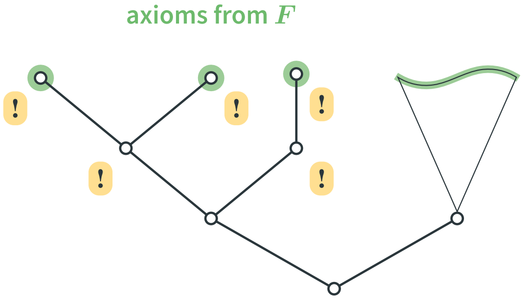
Interpolation by rectification into a resolution proof



Interpolation by rectification into a resolution proof

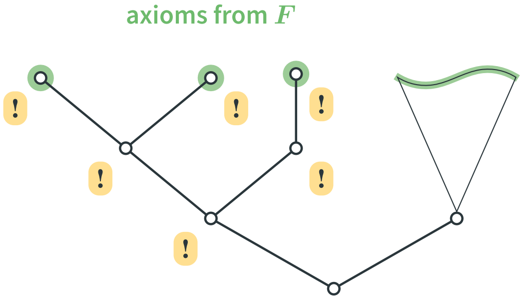


Interpolation by rectification into a resolution proof

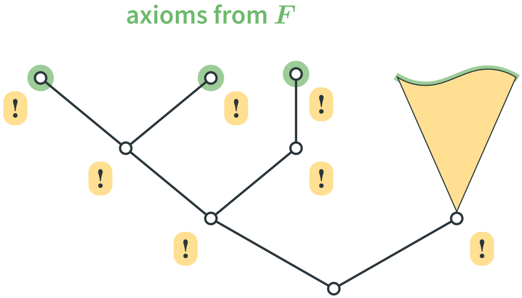


Interpolant generation from DRAT proofs

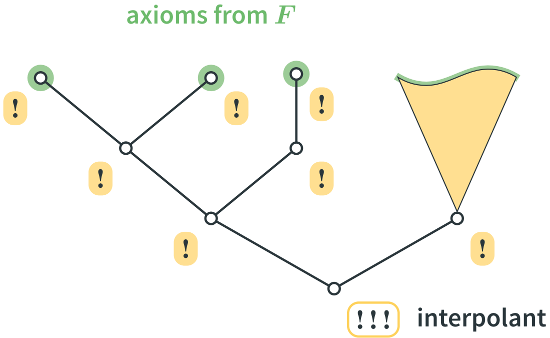
Interpolation by rectification into a resolution proof



Interpolation by rectification into a resolution proof

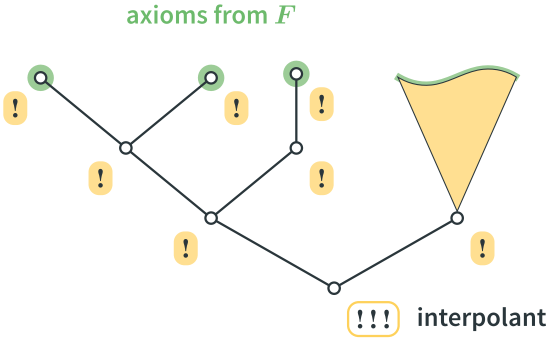


Interpolation by rectification into a resolution proof



Interpolant generation from DRAT proofs

Interpolation by rectification into a resolution proof



Issues

- The interpolant may be exponential with respect to the DRAT proof.
  But DRAT proofs can be exponentially shorter than DRUP proofs!
- Currently we only eliminate RATs and bound paths one by one.
  For a general enough case, the number of required sweeps is reduced.
- Fully rectified DRAT proofs are huge and cannot be held in memory.
  We try to store only necessary information and exploit RUPs to compress it.

Conclusion

Conclusions

- **State-of-the-art SAT solvers do not (and most likely, *will not*) produce resolution proofs, because of inprocessing techniques.**

Conclusions

- State-of-the-art SAT solvers do not (and most likely, *will not*) produce resolution proofs, because of inprocessing techniques.

- The *de facto* standard DRAT certificates can be rectified into resolution proofs, and then interpolants can be extracted.

Conclusions

- State-of-the-art SAT solvers do not (and most likely, *will not*) produce resolution proofs, because of inprocessing techniques.

- The *de facto* standard DRAT certificates can be rectified into resolution proofs, and then interpolants can be extracted.

- Our efforts now are directed towards an efficient implementation of the algorithm by storing minimal information and using restrictive but general enough versions of DRAT.

Backup slides

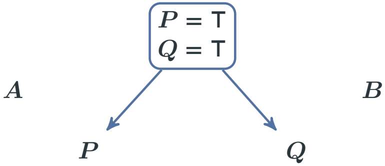
Proofless interpolation

Interpolation through communicating SAT solvers [Chockler Ivrii Matsliah '12]

A B

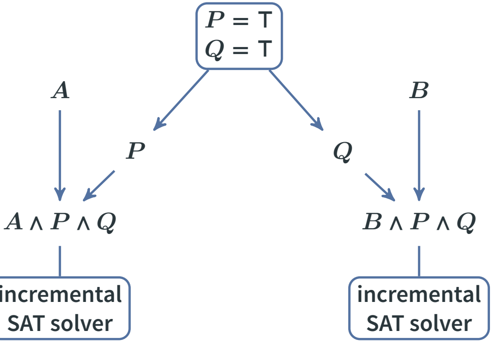
Proofless interpolation

Interpolation through communicating SAT solvers [Chockler Ivrii Matsliah '12]



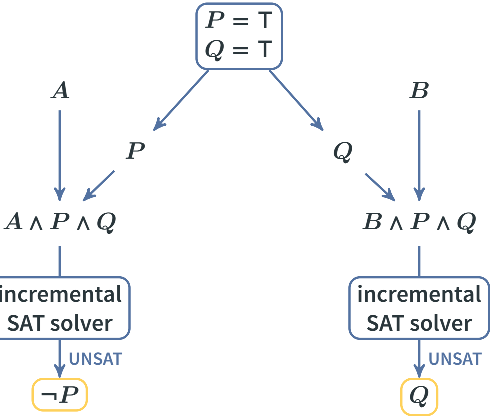
Proofless interpolation

Interpolation through communicating SAT solvers [Chockler Ivrii Matsliah '12]



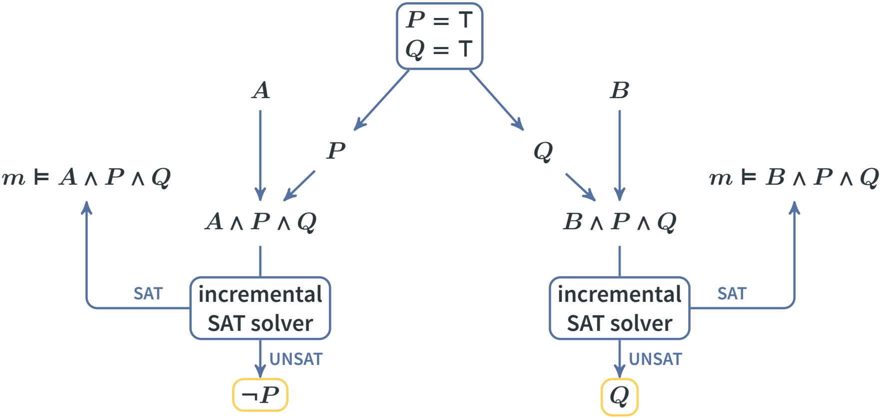
Proofless interpolation

Interpolation through communicating SAT solvers [Chockler Ivrii Matsliah ’12]



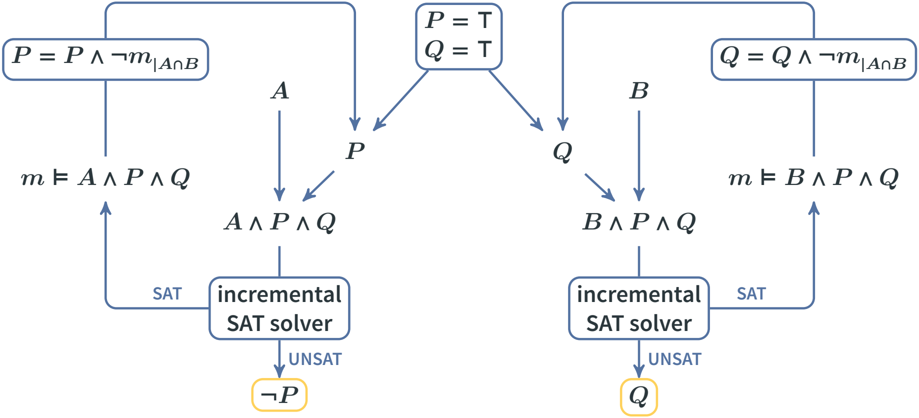
Proofless interpolation

Interpolation through communicating SAT solvers [Chockler Ivrii Matsliah ’12]



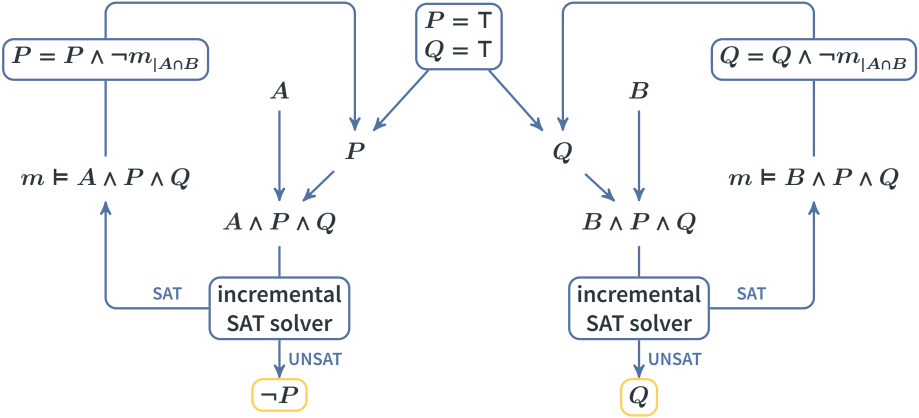
Proofless interpolation

Interpolation through communicating SAT solvers [Chockler Ivrii Matsliah '12]



Proofless interpolation

Interpolation through communicating SAT solvers [Chockler Ivrii Matsliah '12]

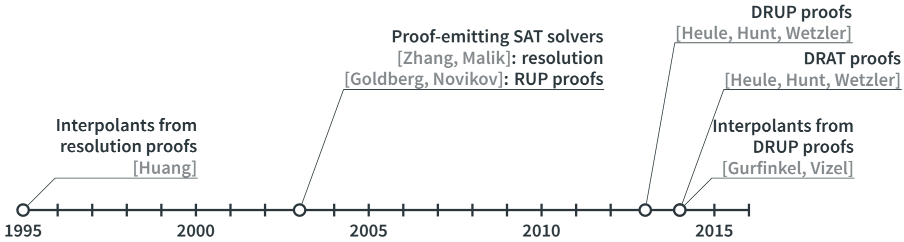


Disadvantages

- Simplification techniques can only be applied locally.
- Obtained interpolants are in DNF or CNF.
- Clause minimization is required to obtain reasonably-sized interpolants.

Proof systems for SAT solvers

A timeline of proof logging and interpolation for SAT solvers

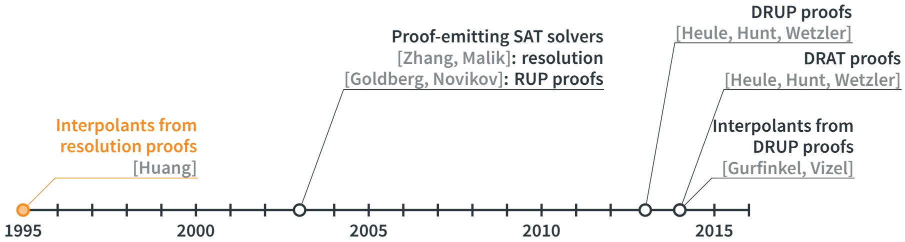


Properties of proof systems

	Resolution	RUP	DRUP	DRAT
Manageable proof size				
Easily expresses CDCL				
Efficient verification				
Expressive enough for inprocessing				
Interpolant generation				

Proof systems for SAT solvers

A timeline of proof logging and interpolation for SAT solvers

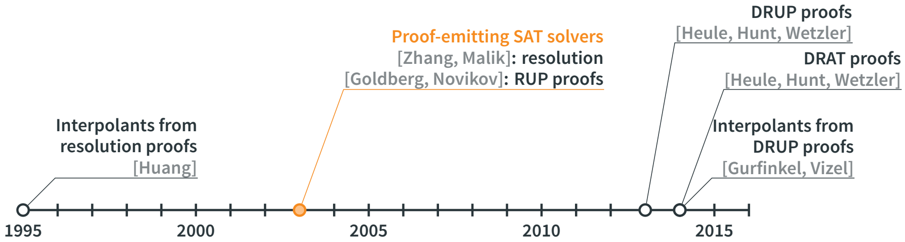


Properties of proof systems

	Resolution	RUP	DRUP	DRAT
Manageable proof size				
Easily expresses CDCL				
Efficient verification				
Expressive enough for inprocessing				
Interpolant generation	✔			

Proof systems for SAT solvers

A timeline of proof logging and interpolation for SAT solvers

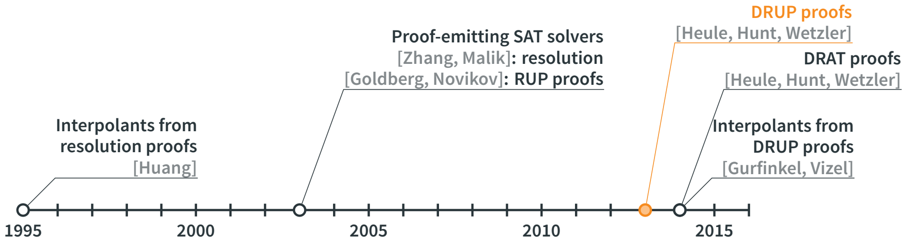


Properties of proof systems

	Resolution	RUP	DRUP	DRAT
Manageable proof size	✗	✓		
Easily expresses CDCL	✗	✓		
Efficient verification	✓	✗		
Expressive enough for inprocessing	✗	✗		
Interpolant generation	✓			

Proof systems for SAT solvers

A timeline of proof logging and interpolation for SAT solvers

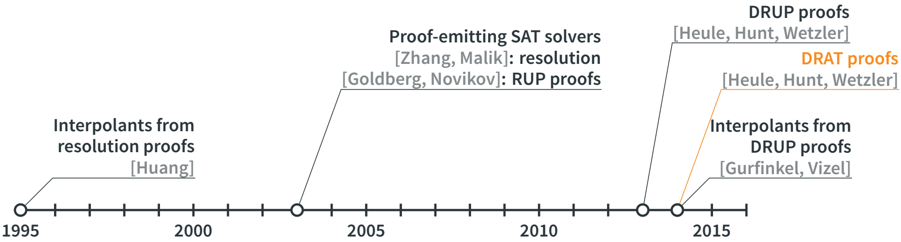


Properties of proof systems

	Resolution	RUP	DRUP	DRAT
Manageable proof size	✗	✓	✓	
Easily expresses CDCL	✗	✓	✓	
Efficient verification	✓	✗	✓	
Expressive enough for inprocessing	✗	✗	✗	
Interpolant generation	✓			

Proof systems for SAT solvers

A timeline of proof logging and interpolation for SAT solvers

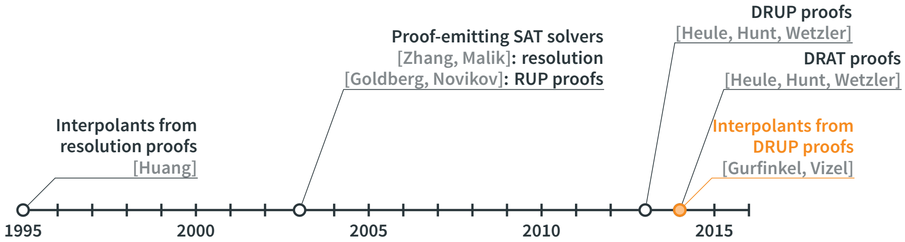


Properties of proof systems

	Resolution	RUP	DRUP	DRAT
Manageable proof size	✘	✔	✔	✔
Easily expresses CDCL	✘	✔	✔	✔
Efficient verification	✔	✘	✔	✔
Expressive enough for inprocessing	✘	✘	✘	✔
Interpolant generation	✔			

Proof systems for SAT solvers

A timeline of proof logging and interpolation for SAT solvers

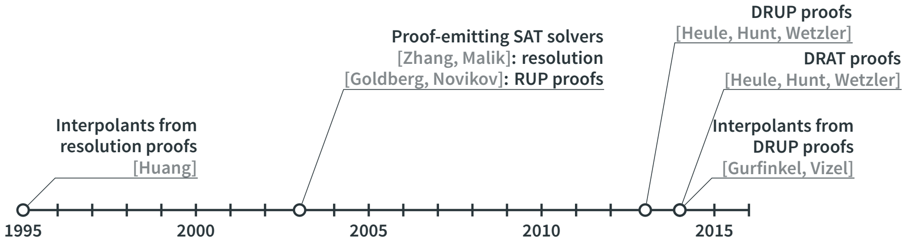


Properties of proof systems

	Resolution	RUP	DRUP	DRAT
Manageable proof size	✗	✓	✓	✓
Easily expresses CDCL	✗	✓	✓	✓
Efficient verification	✓	✗	✓	✓
Expressive enough for inprocessing	✗	✗	✗	✓
Interpolant generation	✓	✓	✓	

Proof systems for SAT solvers

A timeline of proof logging and interpolation for SAT solvers



Properties of proof systems

	Resolution	RUP	DRUP	DRAT
Manageable proof size	✘	✔	✔	✔
Easily expresses CDCL	✘	✔	✔	✔
Efficient verification	✔	✘	✔	✔
Expressive enough for inprocessing	✘	✘	✘	✔
Interpolant generation	✔	✔	✔	???