Labelled Unit Superposition for Instantiation-Based Reasoning

Konstantin Korovin joint work with Christoph Sticksel

SAT/SMT vs First-Order

The problem: Show that a given formula is a theorem.

Ground (SAT/SMT)

$$P(a) \vee f(c) \simeq d$$
$$\neg P(a) \vee Q(d, c)$$

very efficient
not very expressive
DPLL/congruence closure

First-Order

$$\forall x \exists y \;\; Q(x, y) \vee f(x) \not\simeq g(f(y))$$
$$P(a) \vee f(d) \simeq c$$

very expressive
ground: not as efficient
resolution/superposition

From Ground to First-Order: Efficient at ground + Expressive?

Different approaches

Gilmore (1960): generation of ground instances

Robinson (1965): resolution

Plaisted et al (1992): hyper-linking

Weidenbach (1998): splitting in SPASS

Plaisted & Zhu (2000): semantics-based instance generation

Letz & Stenz (2000): disconnection tableaux-type calculus

Riazanov & Voronkov splitting without backtracking

Hooker et al (2002): generation of instances with sem. selection

Baumgartner & Tinelli (2003): ME: Lifting of DPLL

Ganzinger & Korovin (2003): Inst-Gen, modular ground reasoning

Claessen (2005): Equinox

Prevosto & Waldmann (2006): SPASS+T

Navarro & Voronkov (2008): Resolution+Generalization Rule

de Moura & Bjørner (2008): DPLL(T)+Saturation

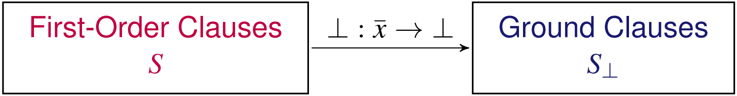
Lynch & Tran (2008): SMELS

Overview of Inst-Gen procedure

First-Order Clauses
S

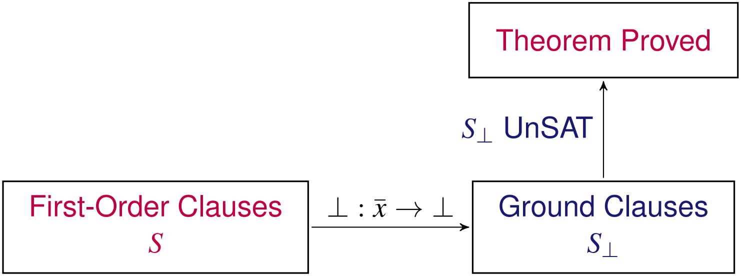
Theorem. This process is sound and complete.

Overview of Inst-Gen procedure



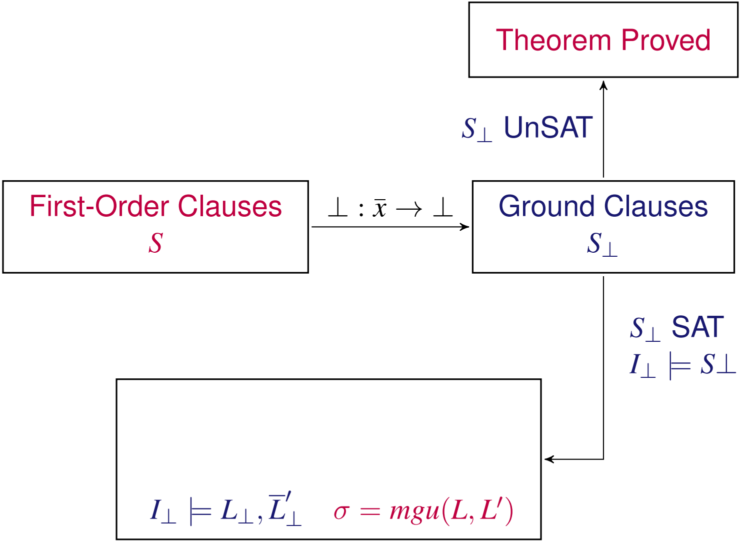
Theorem. This process is sound and complete.

Overview of Inst-Gen procedure



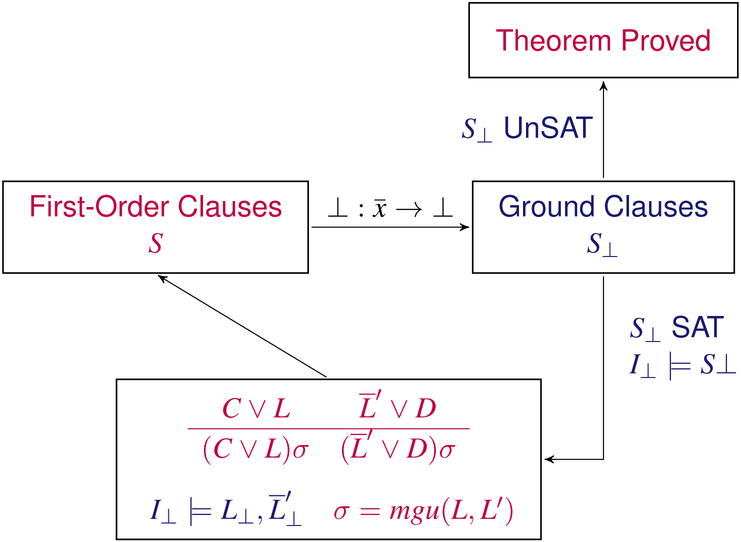
Theorem. This process is sound and complete.

Overview of Inst-Gen procedure



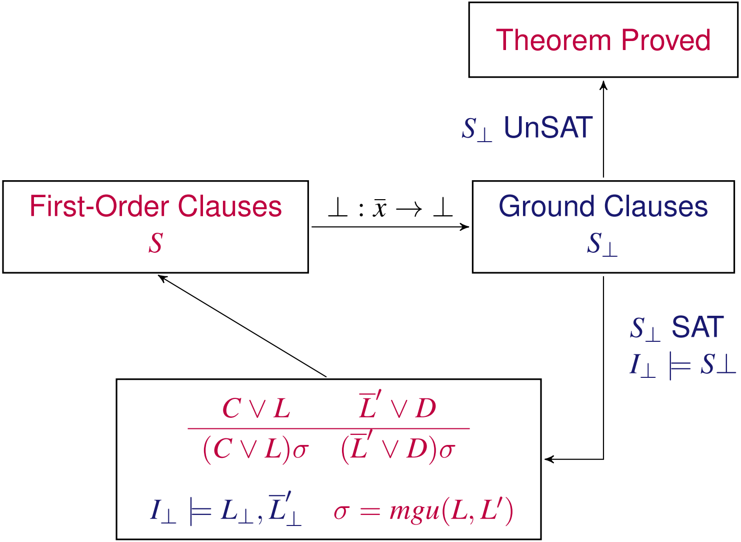
Theorem. This process is sound and complete.

Overview of Inst-Gen procedure



Theorem. This process is sound and complete.

Overview of Inst-Gen procedure



Theorem. This process is sound and complete.

Inst-Gen: Ground Abstraction and Selection

First-order clauses

$$\neg Q(f(x))$$

$$\neg P(f(f(y))$$

$$P(f(z)) \vee Q(z)$$

Ground abstraction with $\bot$

$$\neg Q(f(\bot))$$

$$\neg P(f(f(\bot))$$

$$P(f(\bot)) \vee Q(\bot)$$

- Select literals which are true in ground abstraction

Instantiate:

$$\neg P(f(f(y)))$$

$$P(f(f(y))) \vee Q(f(y))$$

- Ground model has to be refined on the conflict

Inst-Gen: Ground Abstraction and Selection

First-order clauses

$$\neg Q(f(x))$$

$$\neg P(f(f(y))$$

$$P(f(z)) \vee Q(z)$$

Ground abstraction with $\bot$

$$\neg Q(f(\bot))$$

$$\neg P(f(f(\bot))$$

$$P(f(\bot)) \vee Q(\bot)$$

- Select literals which are true in ground abstraction

Instantiate:

$$\neg P(f(f(y)))$$

$$P(f(f(y))) \vee Q(f(y))$$

- Ground model has to be refined on the conflict

Inst-Gen: Ground Abstraction and Selection

First-order clauses

$$\neg Q(f(x))$$

$$\neg P(f(f(y))$$

$$P(f(z)) \lor Q(z)$$

Ground abstraction with $\bot$

$$\underline{\neg Q(f(\bot))}$$

$$\underline{\neg P(f(f(\bot))}$$

$$\underline{P(f(\bot))} \lor Q(\bot)$$

- Select literals which are true in ground abstraction

Instantiate:

$$\neg P(f(f(y)))$$

$$P(f(f(y))) \lor Q(f(y))$$

- Ground model has to be refined on the conflict

Inst-Gen: Ground Abstraction and Selection

First-order clauses

$$\underline{\neg Q(f(x))}$$

$$\underline{\neg P(f(f(y))}$$

$$\underline{P(f(z))} \vee Q(z)$$

Ground abstraction with $\perp$

$$\underline{\neg Q(f(\perp))}$$

$$\underline{\neg P(f(f(\perp))}$$

$$\underline{P(f(\perp))} \vee Q(\perp)$$

- Select literals which are true in ground abstraction

Instantiate:

$$\neg P(f(f(y)))$$

$$P(f(f(y))) \vee Q(f(y))$$

- Ground model has to be refined on the conflict

Inst-Gen: Ground Abstraction and Selection

First-order clauses

$$\underline{\neg Q(f(x))}$$

$$\underline{\neg P(f(f(y))}$$

$$\underline{P(f(z))} \vee Q(z)$$

Ground abstraction with $\perp$

$$\underline{\neg Q(f(\perp))}$$

$$\underline{\neg P(f(f(\perp))}$$

$$\underline{P(f(\perp))} \vee Q(\perp)$$

- Select literals which are true in ground abstraction

Instantiate:

$$\neg P(f(f(y)))$$

$$P(f(f(y))) \vee Q(f(y))$$

- Ground model has to be refined on the conflict

Resolution vs Inst-Gen

$$\textit{Resolution}: \quad \frac{(C \vee L) \qquad (\overline{L}' \vee D)}{(C \vee D)\sigma} \quad \sigma = mgu(L, L')$$

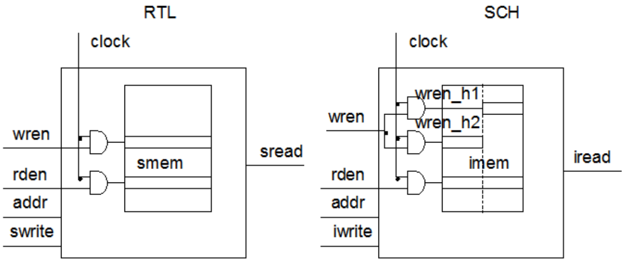
$$\textit{Instantiation}: \quad \frac{(C \vee L) \qquad (\overline{L}' \vee D)}{(C \vee L)\sigma \qquad (\overline{L}' \vee D)\sigma} \quad \sigma = mgu(L, L')$$

Resolution:
ground: not very efficient
EPR: not very efficient
length of clauses can grow fast
recombination of clauses
redundancy elimination

Instantiation:
modular ground reasoning
EPR: efficient
length of clauses is fixed
no recombination
semantic selection
redundancy elim. (res/inst)

Goal: preserve positive features in equational Inst-Gen.

Example: memory verification



Bounded Model Checking:

```
fof(memoryWriteEnabledInsideRange,axiom,
   (nextState(VarCurr,VarNext) => (![AssociatedAddressVar] :
       ((mem_eq_inv_addr_range_1_to_0_addr_assoc(VarNext,AssociatedAddressVar) =>
   (![A] : (((A = AssociatedAddressVar & mem_eq_inv_EXP_10(VarNext)) =>
   (![B] : (((less_5(B) & (~less_0(B))) =>
     (mem_eq_inv_mem2_array(VarNext,A,B) <=> mem_eq_inv_data(VarNext,B))))))))))))).
```

Equality, EPR

Joint work with Zurab Khasidashvili and Andrei Voronkov

Equality Superposition vs Inst-Gen

Superposition

$$\frac{C \vee l \simeq r \quad L[l'] \vee D}{(C \vee D \vee L[r])\theta}$$

ordering restrictions

Instantiation?

$$\frac{C \vee l \simeq r \qquad L[l'] \vee D}{(C \vee l \simeq r)\theta \quad (L[l'] \vee D)\theta}$$

ordering restrictions

Equality Superposition vs Inst-Gen

Superposition

$$\frac{C \vee l \simeq r \quad L[l'] \vee D}{(C \vee D \vee L[r])\theta}$$

ordering restrictions

Instantiation?

$$\frac{C \vee l \simeq r \qquad L[l'] \vee D}{(C \vee l \simeq r)\theta \quad (L[l'] \vee D)\theta}$$

ordering restrictions

Incomplete !

Superposition+Instantiation

$$\begin{array}{rcl} f(h(x)) & \simeq & c \\ h(x) & \simeq & x \\ f(a) & \not\simeq & c \end{array}$$

This set is inconsistent but the contradiction is not deducible by the inference system above.

Superposition+Instantiation

$$
\begin{array}{rcl}
f(h(x)) & \simeq & c \\
h(x) & \simeq & x \\
f(a) & \not\simeq & c
\end{array}
$$

This set is inconsistent but the contradiction is not deducible by the inference system above.

The idea is to consider proofs generated by superposition:

$$
\cfrac{\cfrac{\cfrac{h(x) \simeq x \quad f(h(y)) \simeq c}{f(x) \simeq c} \qquad f(a) \not\simeq c}{c \not\simeq c}}{\square}
$$

Superposition+Instantiation

$$\begin{array}{rcl} f(h(x)) & \simeq & c \\ h(x) & \simeq & x \\ f(a) & \not\simeq & c \end{array}$$

This set is inconsistent but the contradiction is not deducible by the inference system above.

The idea is to consider proofs generated by superposition:

$$\dfrac{\dfrac{\dfrac{h(x) \simeq x \quad f(h(y)) \simeq c}{f(x) \simeq c}\,[x/y] \qquad f(a) \not\simeq c}{c \not\simeq c}\,[a/x]}{\Box}$$

Superposition+Instantiation

$$\begin{array}{rcl} f(h(x)) & \simeq & c \\ h(x) & \simeq & x \\ f(a) & \not\simeq & c \end{array}$$

This set is inconsistent but the contradiction is not deducible by the inference system above.

The idea is to consider proofs generated by superposition:

$$\dfrac{\dfrac{h(x) \simeq x \quad f(h(y)) \simeq c}{f(x) \simeq c}\,[x/y] \qquad f(a) \not\simeq c}{\dfrac{c \not\simeq c}{\square}}\,[a/x]$$

Propagating substitutions: $\{h(a) \simeq a; f(h(a)) \simeq c; f(a) \not\simeq c\}$ ground unsatisfiable.

Superposition+Instantiation

$$
\begin{array}{cccccc}
f(h(x)) & \simeq & c & \vee & C_1(x,y) \\
h(x) & \simeq & x & \vee & C_2(x,y) \\
f(a) & \not\simeq & c & \vee & C_3(x,y)
\end{array}
$$

This set is inconsistent but the contradiction is not deducible by the inference system above.

The idea is to consider proofs generated by superposition:

$$
\cfrac{\cfrac{\cfrac{h(x) \simeq x \quad f(h(y)) \simeq c}{f(x) \simeq c}\,[x/y] \qquad f(a) \not\simeq c}{c \not\simeq c}\,[a/x]}{\square}
$$

Propagating substitutions: $\{h(a) \simeq a; f(h(a)) \simeq c; f(a) \not\simeq c\}$ ground unsatisfiable.

Superposition+Instantiation

$$\begin{array}{ccccc} f(h(x)) & \simeq & c & \vee & C_1(x,y) \\ h(x) & \simeq & x & \vee & C_2(x,y) \\ f(a) & \not\simeq & c & \vee & C_3(x,y) \end{array} \qquad \begin{array}{ccccc} f(h(a)) & \simeq & c & \vee & C_1(a,y) \\ h(a) & \simeq & a & \vee & C_2(a,y) \\ f(a) & \not\simeq & c & \vee & C_3(a,y) \end{array}$$

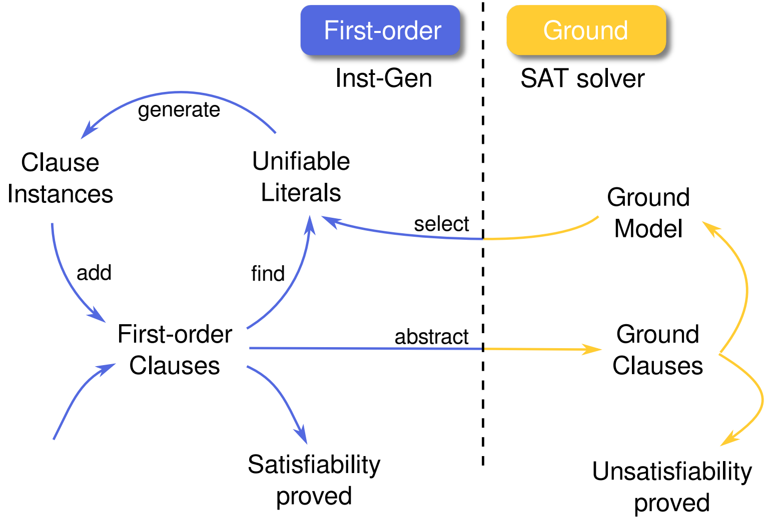
This set is inconsistent but the contradiction is not deducible by the inference system above.

The idea is to consider proofs generated by superposition:

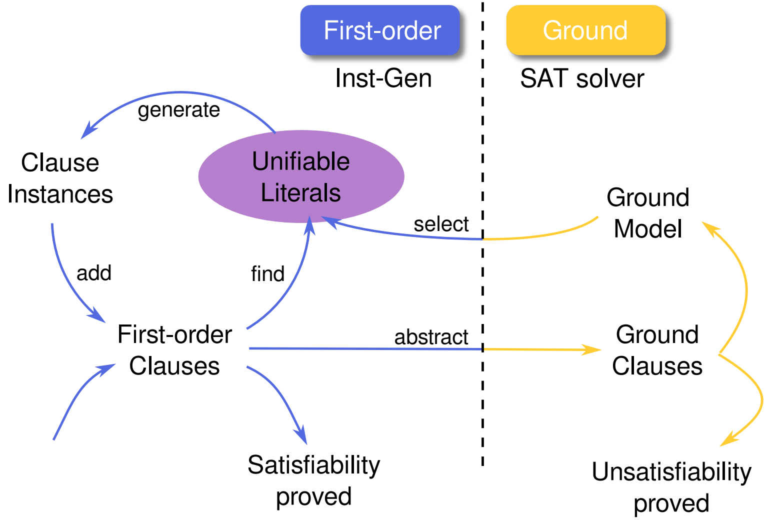
$$\cfrac{\cfrac{\cfrac{h(x) \simeq x \quad f(h(y)) \simeq c}{f(x) \simeq c}\ [x/y] \qquad f(a) \not\simeq c}{c \not\simeq c}\ [a/x]}{\square}$$

Propagating substitutions: $\{h(a) \simeq a; f(h(a)) \simeq c; f(a) \not\simeq c\}$ ground unsatisfiable.

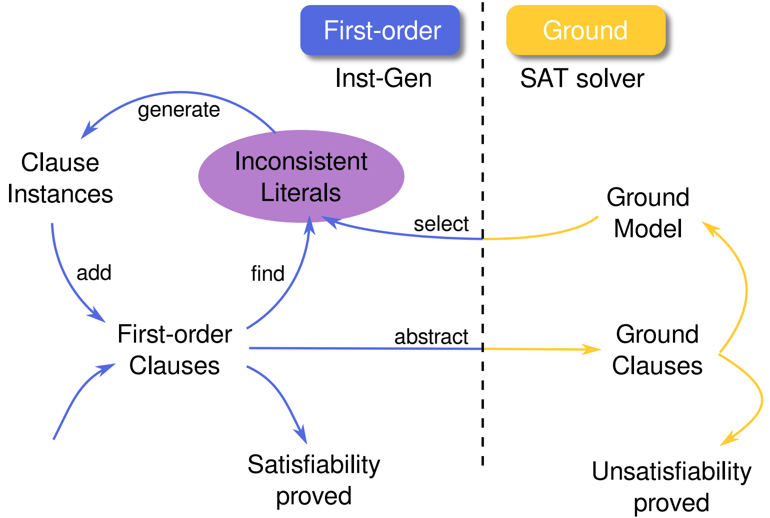
The Inst-Gen Method



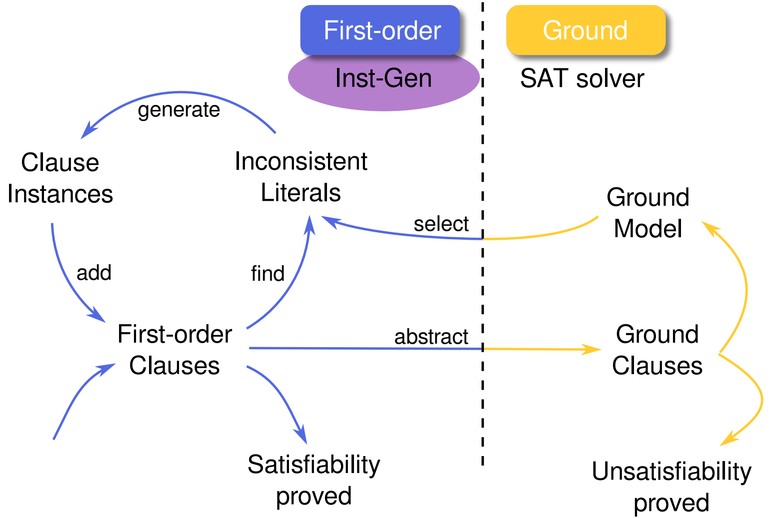
From Inst-Gen to Inst-Gen-Eq



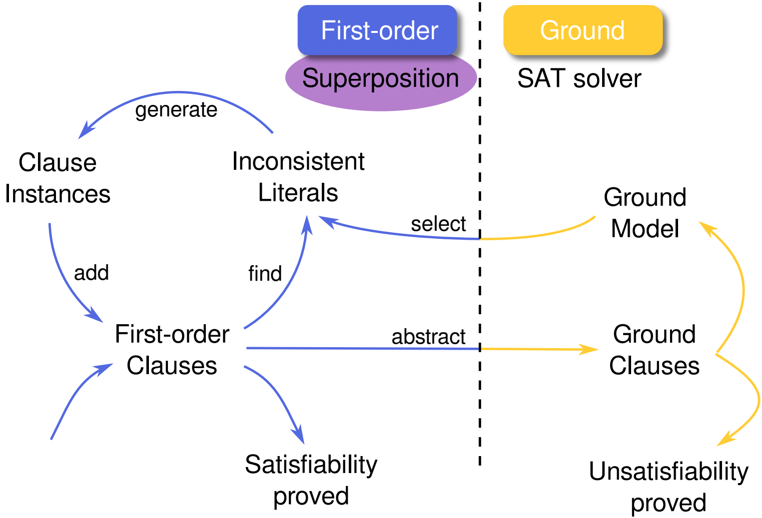
From Inst-Gen to Inst-Gen-Eq



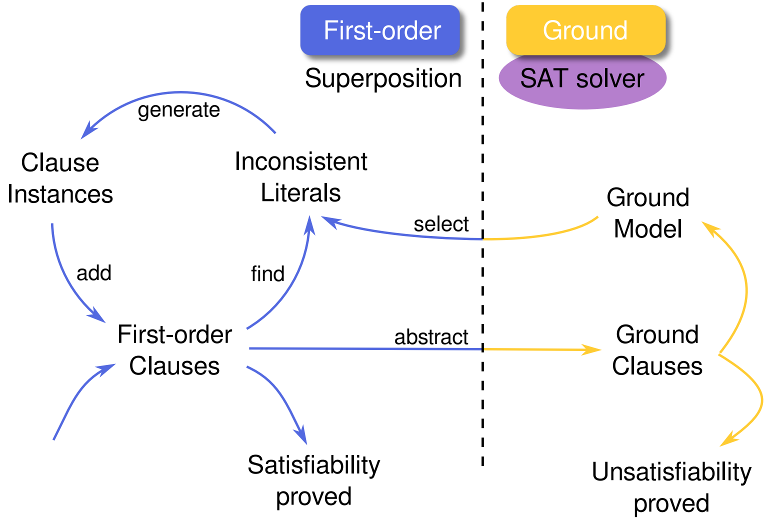
From Inst-Gen to Inst-Gen-Eq



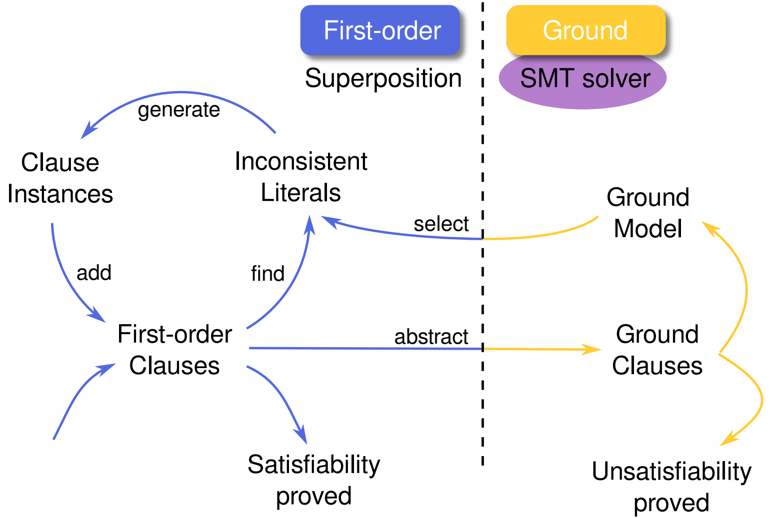
From Inst-Gen to Inst-Gen-Eq



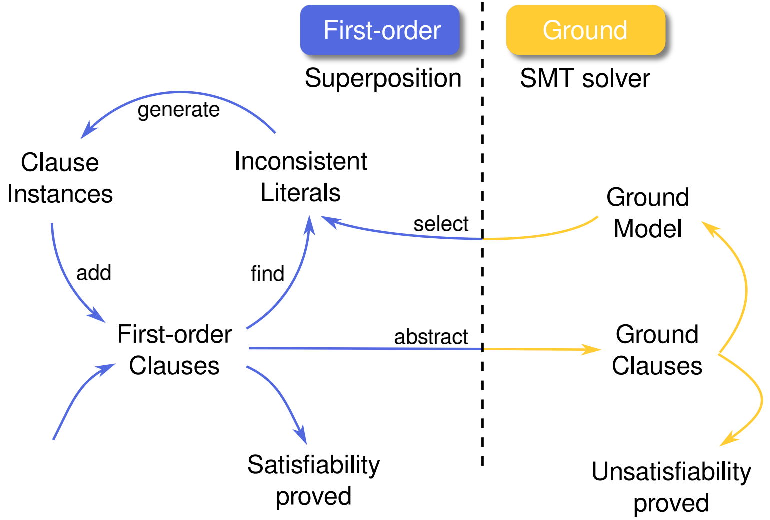
From Inst-Gen to Inst-Gen-Eq



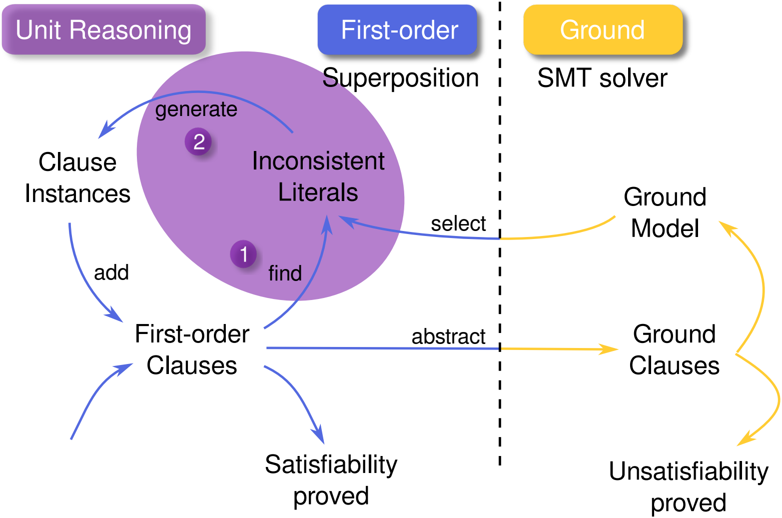
From Inst-Gen to Inst-Gen-Eq



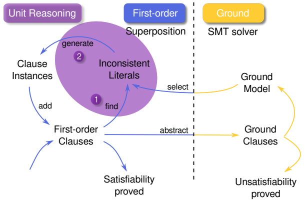
The Inst-Gen-Eq Method



The Inst-Gen-Eq Method



Efficient Unit Reasoning with Selected Literals



Main problems

1. Find inconsistent literals with superposition reasoning
2. Generate clause instances from superposition proofs
3. All (non-redundant) proofs needed for completeness

Our solution

- Labelled Unit Superposition
  - Set labels
  - AND/OR tree labels
  - OBDD labels

Inst-Gen-Eq: (1) Finding Inconsistencies

First-order clauses

$$f(x,y) \simeq f(y,x)$$

$$f(u,v) \not\simeq g(z) \;\vee\; u \simeq z$$

$$f(a,b) \simeq g(c)$$

$$a \not\simeq b$$

Ground abstraction with $\perp$

$$\underline{f(\perp,\perp) \simeq f(\perp,\perp)}$$

$$\underline{f(\perp,\perp) \not\simeq g(\perp)} \;\vee\; \perp \simeq \perp$$

$$\underline{f(a,b) \simeq g(c)}$$

$$\underline{a \not\simeq b}$$

Unit superposition proof: Selected literals inconsistent

$$\dfrac{\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{g(c) \not\simeq g(z)}\,[a/v, b/u]}{\Box}\,[c/z]$$

Inst-Gen-Eq: (1) Finding Inconsistencies

First-order clauses

$$f(x,y) \simeq f(y,x)$$

$$f(u,v) \not\simeq g(z) \ \vee \ u \simeq z$$

$$f(a,b) \simeq g(c)$$

$$a \not\simeq b$$

Ground abstraction with $\bot$

$$\underline{f(\bot,\bot) \simeq f(\bot,\bot)}$$

$$\underline{f(\bot,\bot) \not\simeq g(\bot)} \ \vee \ \bot \simeq \bot$$

$$\underline{f(a,b) \simeq g(c)}$$

$$\underline{a \not\simeq b}$$

Unit superposition proof: Selected literals inconsistent

$$\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}[u/x, v/y]}{\dfrac{g(c) \not\simeq g(z)}{\square}[c/z]}[a/v, b/u]$$

Inst-Gen-Eq: (1) Finding Inconsistencies

First-order clauses

$$\underline{f(x,y) \simeq f(y,x)}$$

$$\underline{f(u,v) \not\simeq g(z)} \;\vee\; u \simeq z$$

$$\underline{f(a,b) \simeq g(c)}$$

$$\underline{a \not\simeq b}$$

Ground abstraction with $\bot$

$$\underline{f(\bot,\bot) \simeq f(\bot,\bot)}$$

$$\underline{f(\bot,\bot) \not\simeq g(\bot)} \;\vee\; \bot \simeq \bot$$

$$\underline{f(a,b) \simeq g(c)}$$

$$\underline{a \not\simeq b}$$

Unit superposition proof: Selected literals inconsistent

$$\cfrac{\cfrac{f(a,b) \simeq g(c) \qquad \cfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{g(c) \not\simeq g(z)}\,[a/v, b/u]}{\square}\,[c/z]$$

Inst-Gen-Eq: (1) Finding Inconsistencies

First-order clauses

$\underline{f(x,y) \simeq f(y,x)}$

$\underline{f(u,v) \not\simeq g(z)} \lor u \simeq z$

$\underline{f(a,b) \simeq g(c)}$

$\underline{a \not\simeq b}$

Ground abstraction with $\perp$

$\underline{f(\perp,\perp) \simeq f(\perp,\perp)}$

$\underline{f(\perp,\perp) \not\simeq g(\perp)} \lor \perp \simeq \perp$

$\underline{f(a,b) \simeq g(c)}$

$\underline{a \not\simeq b}$

Unit superposition proof: Selected literals inconsistent

$$\cfrac{\cfrac{f(a,b) \simeq g(c) \qquad \cfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{g(c) \not\simeq g(z)}\,[a/v, b/u]}{\square}\,[c/z]$$

Inst-Gen-Eq: (2) Generating Instances

Unit superposition proof: Substitution extraction

$$\dfrac{f(a,b)\simeq g(c) \qquad \dfrac{f(x,y)\simeq f(y,x) \qquad f(u,v)\not\simeq g(z)}{f(v,u)\not\simeq g(z)}\,[u/x,v/y]}{\dfrac{g(c)\not\simeq g(z)}{\square}\,[c/z]}\,[a/v,b/u]$$

First-order clauses

$$\underline{f(x,y)\simeq f(y,x)}$$

$$\underline{f(u,v)\not\simeq g(z)} \;\vee\; u\simeq z$$

$$\underline{f(a,b)\simeq g(c)}$$

$$\underline{a\not\simeq b}$$

New first-order instances

$$f(b,a)\simeq f(a,b)$$

$$f(b,a)\not\simeq g(c) \;\vee\; b\simeq c$$

Inst-Gen-Eq: (2) Generating Instances

Unit superposition proof: Substitution extraction

$$\dfrac{\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \quad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{g(c) \not\simeq g(z)}\,[a/v, b/u]}{\square}\,[c/z]$$

First-order clauses

$\underline{f(x,y) \simeq f(y,x)}$

$\underline{f(u,v) \not\simeq g(z)} \ \vee \ u \simeq z$

$\underline{f(a,b) \simeq g(c)}$

$\underline{a \not\simeq b}$

New first-order instances

$f(b,a) \simeq f(a,b)$

$f(b,a) \not\simeq g(c) \ \vee \ b \simeq c$

Inst-Gen-Eq: (2) Generating Instances

Unit superposition proof: Substitution extraction

$$\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{\dfrac{g(c) \not\simeq g(z)}{\square}\,[c/z]}\,[a/v, b/u]$$

First-order clauses

$\underline{f(x,y) \simeq f(y,x)}$

$\underline{f(u,v) \not\simeq g(z)} \;\vee\; u \simeq z$

$\underline{f(a,b) \simeq g(c)}$

$\underline{a \not\simeq b}$

New first-order instances

$f(b,a) \simeq f(a,b)$

$f(b,a) \not\simeq g(c) \;\vee\; b \simeq c$

Inst-Gen-Eq: (2) Generating Instances

Unit superposition proof: Substitution extraction

$$\cfrac{f(a,b) \simeq g(c) \qquad \cfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{\cfrac{g(c) \not\simeq g(z)}{\square}\,[c/z]}\,[a/v, b/u]$$

First-order clauses

$\underline{f(x,y) \simeq f(y,x)}$

$\underline{f(u,v) \not\simeq g(z)} \vee u \simeq z$

$\underline{f(a,b) \simeq g(c)}$

$\underline{a \not\simeq b}$

New first-order instances

$f(b,a) \simeq f(a,b)$

$f(b,a) \not\simeq g(c) \vee b \simeq c$

Inst-Gen-Eq: (2) Generating Instances

Unit superposition proof: Substitution extraction

$$\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\ [u/x, v/y]}{\dfrac{g(c) \not\simeq g(z)}{\square}\ [c/z]}\ [a/v, b/u]$$

First-order clauses

$\underline{f(x,y) \simeq f(y,x)}$

$\underline{f(u,v) \not\simeq g(z)} \ \vee\ u \simeq z$

$\underline{f(a,b) \simeq g(c)}$

$\underline{a \not\simeq b}$

New first-order instances

$f(b,a) \simeq f(a,b)$

$f(b,a) \not\simeq g(c) \ \vee\ b \simeq c$

Inst-Gen-Eq: (3) Many Proofs

Proof of inconsistency (1)

$$\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{\dfrac{g(c) \not\simeq g(z)}{\square}\,[c/z]}\,[a/v, b/u]$$

Proof of inconsistency (2)

$$\dfrac{\dfrac{f(a,b) \simeq g(c) \qquad f(u,v) \not\simeq g(z)}{g(c) \not\simeq g(z)}\,[a/u, b/v]}{\square}\,[c/z]$$

Instances from proof (1)

$$f(b,a) \simeq f(a,b)$$
$$f(b,a) \not\simeq g(c) \lor b \simeq c$$

Instances from proof (2)

$$f(a,b) \not\simeq g(c) \lor a \simeq c$$

Inst-Gen-Eq: (3) Many Proofs

Proof of inconsistency (1)

$$\dfrac{f(a,b) \simeq g(c) \qquad \dfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{\dfrac{g(c) \not\simeq g(z)}{\Box}\,[c/z]}\,[a/v, b/u]$$

Proof of inconsistency (2)

$$\dfrac{f(a,b) \simeq g(c) \qquad f(u,v) \not\simeq g(z)}{\dfrac{g(c) \not\simeq g(z)}{\Box}\,[c/z]}\,[a/u, b/v]$$

Instances from proof (1)

$$f(b,a) \simeq f(a,b)$$
$$f(b,a) \not\simeq g(c) \lor b \simeq c$$

Instances from proof (2)

$$f(a,b) \not\simeq g(c) \lor a \simeq c$$

Inst-Gen-Eq: (3) Many Proofs

Proof of inconsistency (1)

$$\cfrac{\cfrac{f(a,b)\simeq g(c) \qquad \cfrac{f(x,y)\simeq f(y,x) \qquad f(u,v)\not\simeq g(z)}{f(v,u)\not\simeq g(z)}\,[u/x,v/y]}{g(c)\not\simeq g(z)}\,[a/v,b/u]}{\square}\,[c/z]$$

Proof of inconsistency (2)

$$\cfrac{\cfrac{f(a,b)\simeq g(c) \qquad f(u,v)\not\simeq g(z)}{g(c)\not\simeq g(z)}\,[a/u,b/v]}{\square}\,[c/z]$$

Instances from proof (1)

$$f(b,a)\simeq f(a,b)$$
$$f(b,a)\not\simeq g(c)\vee b\simeq c$$

Instances from proof (2)

$$f(a,b)\not\simeq g(c)\vee a\simeq c$$

Inst-Gen-Eq: (3) Many Proofs

Proof of inconsistency (1)

$$\cfrac{\cfrac{f(a,b) \simeq g(c) \qquad \cfrac{f(x,y) \simeq f(y,x) \qquad f(u,v) \not\simeq g(z)}{f(v,u) \not\simeq g(z)}\,[u/x, v/y]}{g(c) \not\simeq g(z)}\,[a/v, b/u]}{\square}\,[c/z]$$

Proof of inconsistency (2)

$$\cfrac{\cfrac{f(a,b) \simeq g(c) \qquad f(u,v) \not\simeq g(z)}{g(c) \not\simeq g(z)}\,[a/u, b/v]}{\square}\,[c/z]$$

Instances from proof (1)

$$f(b,a) \simeq f(a,b)$$

$$f(b,a) \not\simeq g(c) \vee b \simeq c$$

Instances from proof (2)

$$f(a,b) \not\simeq g(c) \vee a \simeq c$$

The Labelling Approach

Informally: $\{\ldots, C \cdot \theta, \ldots\} : L$ then

- C is at the leaf of the proof of L and
- θ is the accumulated substitution.

Set Label is a set of closures $\mathcal{T} = \{C \cdot \theta_1, \ldots, C_n \cdot \theta_n\}$

Closure: $C \cdot \theta$, clause C and substitution θ

Initial labels: $\{C \cdot []\} : L$ where L is selected in C

$$\{\underline{f(u,v) \not\simeq g(z)} \ \vee \ u \simeq z \cdot []\} : f(u,v) \not\simeq g(z)$$

Important: $C \cdot \theta$ can become redundant.

The Labelling Approach

Informally: $\{\dots, C \cdot \theta, \dots\} : L$ then

- C is at the leaf of the proof of L and
- θ is the accumulated substitution.

Set Label is a set of closures $\mathcal{T} = \{C \cdot \theta_1, \dots, C_n \cdot \theta_n\}$

Closure: $C \cdot \theta$, clause C and substitution θ

Initial labels: $\{C \cdot []\} : L$ where L is selected in C

$$\{\underline{f(u,v) \not\simeq g(z)} \ \vee \ u \simeq z \cdot []\} : f(u,v) \not\simeq g(z)$$

Important: $C \cdot \theta$ can become redundant.

Inference Rules in Labelled Unit Superposition

Labelled Superposition

$$\frac{\mathcal{T} : l \simeq r \qquad \mathcal{T}' : L[l']}{(\mathcal{T} \sqcap \mathcal{T}')\sigma : L[r]\sigma} \; (\sigma)$$

$\sigma = mgu(l, l')$,
ordering restrictions

Variant merging

$$\frac{\mathcal{T} : L \qquad \mathcal{T}' : L'}{\mathcal{T} \sqcup \mathcal{T}'\sigma : L} \; (\sigma)$$

$L = L'\sigma$,
σ is a renaming

Equality resolution

$$\frac{\mathcal{T} : (l \not\simeq r)}{\mathcal{T}\sigma : \Box} \; (\sigma)$$

$\sigma = mgu(l, r)$

- No labels in side conditions
- $\sqcap$ and $\sqcup$ dependant on implementation of labels
- Label $\mathcal{T}$ is either a set, an AND/OR tree or an OBDD

Set Labelled Unit Superposition

- Label is a set of closures
- Set union $\cup$ in both merging $\sqcup$ and superposition $\sqcap$

Superposition

$$\frac{\{C \cdot []\} : f(x,y) \simeq f(y,x) \quad \{D \cdot []\} : f(u,v) \not\simeq g(z)}{\{C \cdot [u/x, v/y], D \cdot []\} : f(v,u) \not\simeq g(z)} \; [u/x, v/y]$$

Merging $f(u,v) \not\simeq g(z)$ and $f(v,u) \not\simeq g(z)$ with $[u/v, v/u]$

$$\{D \cdot [], C \cdot [v/x, u/y], D \cdot [u/v, v/u]\} : f(u,v) \not\simeq g(z)$$

Label of the contradiction $\square$

$$\{D \cdot [a/u, b/v, c/z], E \cdot [], C \cdot [b/x, a/y], D \cdot [b/u, a/v, c/z]\}$$

Set Labelled Unit Superposition

- Label is a set of closures
- Set union $\cup$ in both merging $\sqcup$ and superposition $\sqcap$

Superposition

$$\frac{\{C \cdot []\} : f(x,y) \simeq f(y,x) \quad \{D \cdot []\} : f(u,v) \not\simeq g(z)}{\{C \cdot [u/x, v/y], D \cdot []\} : f(v,u) \not\simeq g(z)} \; [u/x, v/y]$$

Merging $f(u,v) \not\simeq g(z)$ and $f(v,u) \not\simeq g(z)$ with $[u/v, v/u]$

$$\{D \cdot [], C \cdot [v/x, u/y], D \cdot [u/v, v/u]\} : f(u,v) \not\simeq g(z)$$

Label of the contradiction $\square$

$$\{D \cdot [a/u, b/v, c/z], E \cdot [], C \cdot [b/x, a/y], D \cdot [b/u, a/v, c/z]\}$$

Set Labelled Unit Superposition

- Label is a set of closures
- Set union $\cup$ in both merging $\sqcup$ and superposition $\sqcap$

Superposition

$$\frac{\{C \cdot []\} : f(x,y) \simeq f(y,x) \quad \{D \cdot []\} : f(u,v) \not\simeq g(z)}{\{C \cdot [u/x, v/y], D \cdot []\} : f(v,u) \not\simeq g(z)} \; [u/x, v/y]$$

Merging $f(u,v) \not\simeq g(z)$ and $f(v,u) \not\simeq g(z)$ with $[u/v, v/u]$

$$\{D \cdot [], C \cdot [v/x, u/y], D \cdot [u/v, v/u]\} : f(u,v) \not\simeq g(z)$$

Label of the contradiction $\square$

$$\{D \cdot [a/u, b/v, c/z], E \cdot [], C \cdot [b/x, a/y], D \cdot [b/u, a/v, c/z]\}$$

Set Labelled Unit Superposition

- Label is a set of closures
- Set union $\cup$ in both merging $\sqcup$ and superposition $\sqcap$

Superposition

$$\frac{\{C \cdot []\} : f(x,y) \simeq f(y,x) \quad \{D \cdot []\} : f(u,v) \not\simeq g(z)}{\{C \cdot [u/x, v/y], D \cdot []\} : f(v,u) \not\simeq g(z)} \; [u/x, v/y]$$

Merging $f(u,v) \not\simeq g(z)$ and $f(v,u) \not\simeq g(z)$ with $[u/v, v/u]$

$$\{D \cdot [], C \cdot [v/x, u/y], D \cdot [u/v, v/u]\} : f(u,v) \not\simeq g(z)$$

Label of the contradiction $\square$

$$\{D \cdot [a/u, b/v, c/z], E \cdot [], C \cdot [b/x, a/y], D \cdot [b/u, a/v, c/z]\}$$

Set Labelled Unit Superposition

- Label is a set of closures
- Set union $\cup$ in both merging $\sqcup$ and superposition $\sqcap$

Superposition

$$\frac{\{C \cdot []\} : f(x,y) \simeq f(y,x) \quad \{D \cdot []\} : f(u,v) \not\simeq g(z)}{\{C \cdot [u/x, v/y], D \cdot []\} : f(v,u) \not\simeq g(z)} \; [u/x, v/y]$$

Merging $f(u,v) \not\simeq g(z)$ and $f(v,u) \not\simeq g(z)$ with $[u/v, v/u]$

$$\{D \cdot [], C \cdot [v/x, u/y], D \cdot [u/v, v/u]\} : f(u,v) \not\simeq g(z)$$

Label of the contradiction $\square$

$$\{D \cdot [a/u, b/v, c/z], E \cdot [], C \cdot [b/x, a/y], D \cdot [b/u, a/v, c/z]\}$$

Set Labelled Unit Superposition

- Label is a set of closures
- Set union $\cup$ in both merging $\sqcup$ and superposition $\sqcap$

Superposition

$$\frac{\{C \cdot []\} : f(x,y) \simeq f(y,x) \quad \{D \cdot []\} : f(u,v) \not\simeq g(z)}{\{C \cdot [u/x, v/y], D \cdot []\} : f(v,u) \not\simeq g(z)} \; [u/x, v/y]$$

Merging $f(u,v) \not\simeq g(z)$ and $f(v,u) \not\simeq g(z)$ with $[u/v, v/u]$

$$\{D \cdot [], C \cdot [v/x, u/y], D \cdot [u/v, v/u]\} : f(u,v) \not\simeq g(z)$$

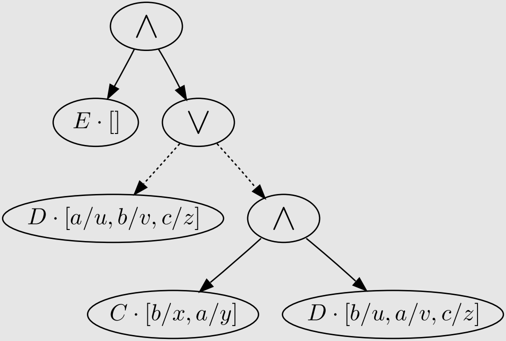
Label of the contradiction $\Box$

$$\{D \cdot [a/u, b/v, c/z], E \cdot [], E \cdot [], C \cdot [b/x, a/y], D \cdot [b/u, a/v, c/z]\}$$

Tree Labelled Unit Superposition

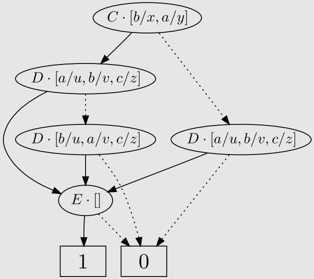
- Preserve Boolean structure of proofs
- Closure is a propositional variable in an AND/OR tree
- Conjunction $\wedge$ in superposition, disjunction $\vee$ in merging

Label of the Contradiction $\square$



OBDD Labelled Unit Superposition

Label of the contradiction $\square$



Disadvantages of trees

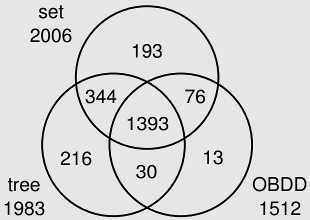
- Not produced in normal form
- Sequence of inferences determines shape
- Potential growth *ad infinitum*

- OBDD as normal form
- Maintenance effort
- Reordering required

Evaluation: Sets vs. Trees vs. OBDDs

iProver-Eq – CVC3 as a background solver.

Solved equational problems



Features

	Normal form	Precise elim.
Sets	yes	no
Trees	no	yes
OBDDs	yes	yes

Summary

Instantiation-based reasoning Inst-Gen-Eq

- labelled unit superposition for instantiation
- simultaneous proofs with all literal variants
- different label structures: sets, trees, OBDDs
- implementation in iProver-Eq

Current/Future Work

- demodulation
- hybrid labels
- linear arithmetic: Inst-Gen+LASCA
- EPR optimizations