Quantifier Simplification by Unification in SMT

FroCoS 2021

Pascal Fontaine[1], **Hans-Jörg Schurr**[2]

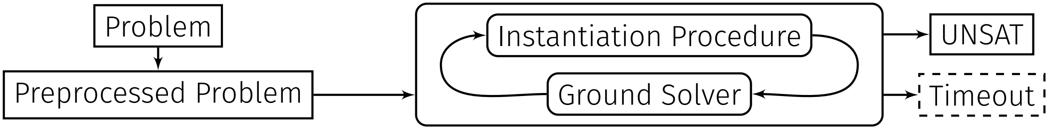
[1]Université de Liège

[2]University of Lorraine, CNRS, Inria, and LORIA

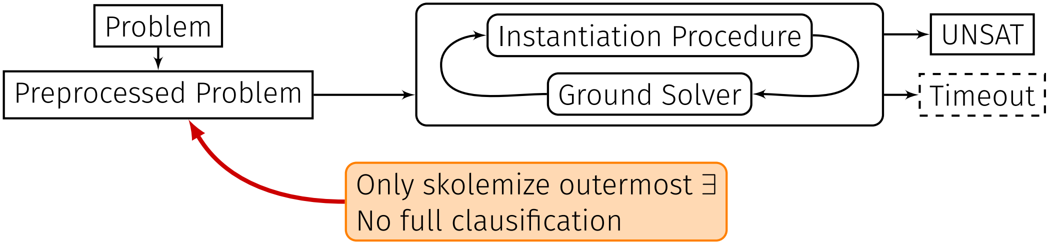
September 9, 2021

- Traditional CDCL(T) based SMT solver.
- Only refutations for quantified problems.
- Proof producing and integrated in Isabelle/HOL.

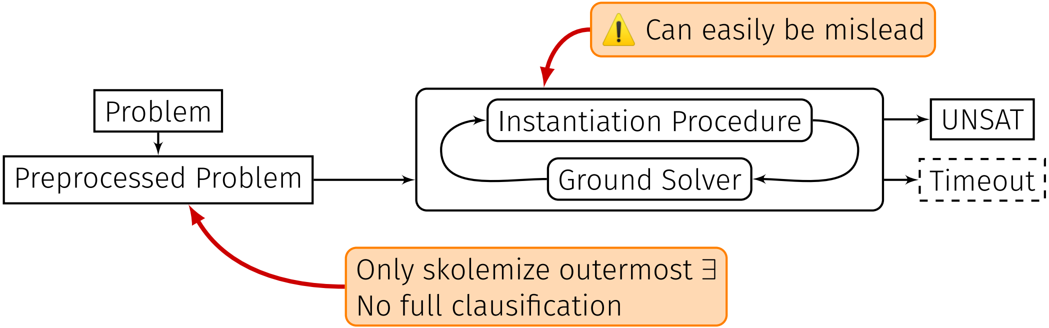
The Instantiation Loop



The Instantiation Loop



The Instantiation Loop



An Example

$$\forall x.\, P(x) \rightarrow P(f(x, c))$$
$$\forall y.\, (\forall z.\, P(z) \rightarrow P(f(z, y))) \rightarrow \neg P(y)$$
$$P(c)$$

An Example

Lemma

$$\forall x.\, P(x) \rightarrow P(f(x, c))$$
$$\forall y.\, (\forall z.\, P(z) \rightarrow P(f(z, y))) \rightarrow \neg P(y)$$
$$P(c)$$

An Example

Lemma

$$\forall x.\, P(x) \to P(f(x, c))$$

$$\forall y.\, (\forall z.\, P(z) \to P(f(z, y))) \to \neg P(y)$$

$$P(c)$$

Using the lemma

An Example

$$\forall x.\, P(x) \to P(f(x, c))$$

$$\forall y.\, (\forall z.\, P(z) \to P(f(z, y))) \to \neg P(y)$$

$$P(c)$$

An Example

Instantiate with c

$$\forall x.\, P(x) \rightarrow P(f(x, c))$$

$$\forall y.\, (\forall z.\, P(z) \rightarrow P(f(z, y))) \rightarrow \neg P(y)$$

$$P(c)$$

An Example

$$\forall x.\, P(x) \to P(f(x, c))$$

$$(\forall z.\, P(z) \to P(f(z, c))) \to \neg P(c)$$

$$P(c)$$

An Example

$$\forall x.\, P(x) \rightarrow P(f(x, c))$$

$$(\forall z.\, P(z) \rightarrow P(f(z, c))) \rightarrow \neg P(c)$$

$$P(c)$$

Skolemize z

An Example

$$\forall x.\, P(x) \rightarrow P(f(x, c))$$

$$P(s_1) \rightarrow P(f(s_1, c)) \quad \rightarrow \neg P(c)$$

$$P(c)$$

An Example

$$\forall x.\, P(x) \to P(f(x, c))$$

$$P(s_1) \to P(f(s_1, c)) \quad \to \neg P(c)$$

$$P(c)$$

An Example

Instantiate with s_1

$$\forall x.\, P(x) \to P(f(x, c))$$

$$P(s_1) \to P(f(s_1, c)) \quad \to \neg P(c)$$

$$P(c)$$

An Example

$$P(s_1) \to P(f(s_1, c))$$

$$P(s_1) \to P(f(s_1, c)) \quad \to \neg P(c)$$

$$P(c)$$

Let's use Unification

$$\forall x.\, P(x) \to P(f(x,c))$$

$$\forall y.\, (\forall z.\, P(z) \to P(f(z,y))) \to \neg P(y)$$

$$P(c)$$

Let's use Unification

$$\forall x.\, P(x) \to P(f(x, c))$$

$$\forall y.\, (P(s_1(y)) \to P(f(s_1(y), y))) \to \neg P(y)$$

$$P(c)$$

Let's use Unification

$$\forall x.\, P(x) \to P(f(x, c))$$
$$\forall y.\, (P(s_1(y)) \to P(f(s_1(y), y))) \to \neg P(y)$$
$$P(c)$$

Unifier: $y \mapsto c$, $x \mapsto s_1(c)$

Let's use Unification

$$P(s_1(c)) \to P(f(s_1(c), c))$$
$$(P(s_1(c)) \to P(f(s_1(c), c)) \to \neg P(c)$$
$$P(c)$$

Unifier: $y \mapsto c$, $x \mapsto s_1(c)$

Add: $\top \to \neg P(c)$

Let's use Unification

$$P(s_1(c)) \to P(f(s_1(c), c))$$
$$(P(s_1(c)) \to P(f(s_1(c), c)) \to \neg P(c)$$
$$P(c)$$

Unifier: $y \mapsto c$, $x \mapsto s_1(c)$

Add: $\top \to \neg P(c)$

The General Rule

$$\frac{\forall x_1, \ldots, x_n .\, \psi_1 \qquad \forall x_{n+1}, \ldots, x_m .\, \varphi[Qy_1, \ldots, y_o .\, \psi_2]}{\forall x_{k_1}, \ldots, x_{k_j} .\, \varphi[b]\sigma}$$

The General Rule

$$\frac{\forall x_1, \ldots, x_n.\, \psi_1 \qquad \forall x_{n+1}, \ldots, x_m.\, \varphi[Qy_1, \ldots, y_o.\, \psi_2]}{\forall x_{k_1}, \ldots, x_{k_j}.\, \varphi[b]\sigma}$$

- $\top$ if the polarities of ψ_1 and ψ_2 is equal
- $\bot$ if the polarities of ψ_1 and ψ_2 is different

The General Rule

$Q \in \{\forall, \exists\}$
first nested quantifier

$$\frac{\forall x_1, \ldots, x_n.\, \psi_1 \qquad \forall x_{n+1}, \ldots, x_m.\, \varphi[Qy_1, \ldots, y_o.\, \psi_2]}{\forall x_{k_1}, \ldots, x_{k_j}.\, \varphi[b]\sigma}$$

- $\top$ if the polarities of ψ_1 and ψ_2 is equal
- $\bot$ if the polarities of ψ_1 and ψ_2 is different

After Skolemization,
ψ_1 and ψ_2 must be unifiable.

$$\frac{\forall x_1, \ldots, x_n.\, \psi_1 \qquad \forall x_{n+1}, \ldots, x_m.\, \varphi[Qy_1, \ldots, y_o.\, \psi_2]}{\forall x_{k_1}, \ldots, x_{k_j}.\, \varphi[b]\sigma}$$

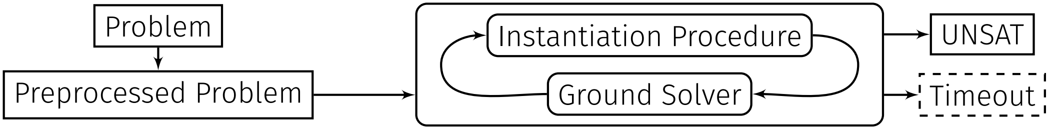
- $\top$ if the polarities of ψ_1 and ψ_2 is equal
- $\bot$ if the polarities of ψ_1 and ψ_2 is different

After Skolemization, ψ_1 and ψ_2 must be unifiable.

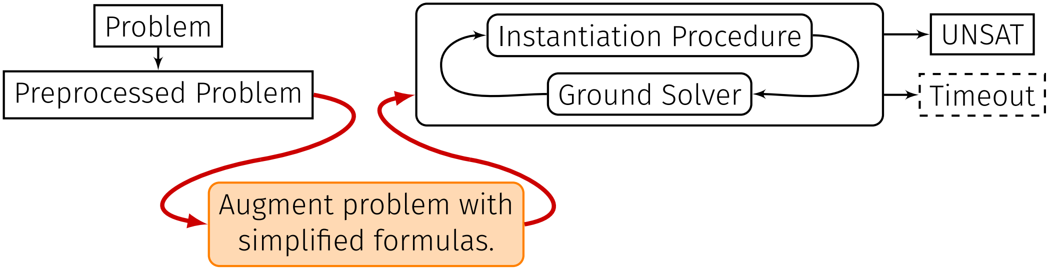
$$\frac{\forall x_1, \ldots, x_n .\ \psi_1 \qquad \forall x_{n+1}, \ldots, x_m .\ \varphi[Q y_1, \ldots, y_o .\ \psi_2]}{\forall x_{k_1}, \ldots, x_{k_j} .\ \varphi[b]\sigma}$$

Unifier

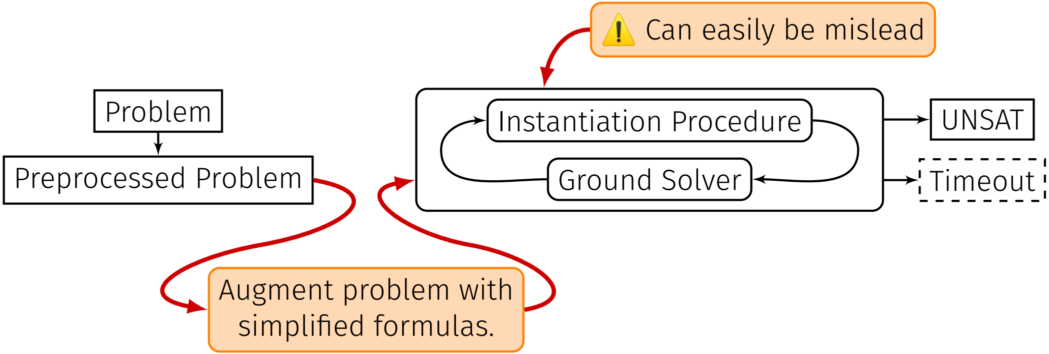
- $\top$ if the polarities of ψ_1 and ψ_2 is equal
- $\bot$ if the polarities of ψ_1 and ψ_2 is different


Problem
Preprocessed Problem
Instantiation Procedure
Ground Solver
UNSAT
Timeout

The Instantiation Loop



The Instantiation Loop



Implementation

- We have to perform many unifiability tests.
- We can steal the standard index data structures used by theorem provers.
- In our case: a non-perfect discrimination tree
- and a subsequent unifiability check.
- By treating strongly quantified variables as constants we can avoid creating any new symbols for skolemization!

Implementation

- We have to perform many unifiability tests.
- We can steal the standard index data structures used by theorem provers.
- In our case: a non-perfect discrimination tree
- and a subsequent unifiability check.
- By treating strongly quantified variables as constants we can avoid creating any new symbols for skolemization!

Variants

We implemented multiple variants of the base rule:

1. *Eager*: remove subformulas even if they don't start with a quantifier.
2. *Deletion*: remove the simplified formula.
3. *Eager+Deletion*: Both of the ones above.
4. *Solitary Variable*: remove subformulas containing a variable that occurs in no other subformula.
5. *Solitary Variable+Deletion*

Variants

We implemented multiple variants of the base rule:

1. *Eager*: remove subformulas even if they don't start with a quantifier.
2. *Deletion*: remove the simplified formula.
3. *Eager+Deletion*: Both of the ones above.
4. *Solitary Variable*: remove subformulas containing a variable that occurs in no other subformula.
5. *Solitary Variable+Deletion*

Variants

We implemented multiple variants of the base rule:

1. *Eager*: remove subformulas even if they don't start with a quantifier.
2. *Deletion*: remove the simplified formula.
3. *Eager+Deletion*: Both of the ones above.
4. *Solitary Variable*: remove subformulas containing a variable that occurs in no other subformula.
5. *Solitary Variable+Deletion*

Experimental Results: Baseline Strategies

vs. Default (solves 31 690)	N	E	S	Nd	Ed	Sd	Total
Solved	31 927	31 772	31 928	31 733	21 405	21 823	32 151
	+237	+82	**+238**	+43	−10 285	−9 867	+461
Gained	282	**315**	285	291	115	255	475
Lost	**45**	233	47	248	10 400	10 122	14
vs. Theoretical Best (solves 32 633)							
Gained	83	80	85	**86**	32	76	**125**

180 s timeout, 38 717 benchmarks, unsat. only
ALIA, AUFLIA, AUFLIRA, UF, UFIDL, UFLIA, UFLRA

N is Normal, **E** is Eager, **S** is Solitary Variable, **d** is Deletion

Experimental Results: Baseline Strategies

vs. Default (solves 31 690)	N	E	S	Nd	Ed	Sd	Total
Solved	31 927	31 772	31 928	31 733	21 405	21 823	32 151
	+237	+82	**+238**	+43	−10 285	−9 867	+461
Gained	282	**315**	285	291	115	255	475
Lost	**45**	233	47	248	10 400	10 122	14
vs. Theoretical Best (solves 32 633)							
Gained	83	80	85	**86**	32	76	**125**

180 s timeout, 38 717 benchmarks, unsat. only
ALIA, AUFLIA, AUFLIRA, UF, UFIDL, UFLIA, UFLRA

N is Normal, **E** is Eager, **S** is Solitary Variable, **d** is Deletion

Experimental Results: Baseline Strategies

vs. Default (solves 31 690)	N	E	S	Nd	Ed	Sd	Total
Solved	31 927	31 772	31 928	31 733	21 405	21 823	32 151
	+237	+82	**+238**	+43	−10 285	−9 867	+461
Gained	282	**315**	285	291	115	255	475
Lost	**45**	233	47	248	10 400	10 122	14
vs. Theoretical Best (solves 32 633)							
Gained	83	80	85	**86**	32	76	**125**

180 s timeout, 38 717 benchmarks, unsat. only
ALIA, AUFLIA, AUFLIRA, UF, UFIDL, UFLIA, UFLRA

N is Normal, **E** is Eager, **S** is Solitary Variable, **d** is Deletion

Experimental Results: Baseline Strategies

vs. Default (solves 31 690)	N	E	S	Nd	Ed	Sd	Total
Solved	31 927	31 772	31 928	31 733	21 405	21 823	32 151
	+237	+82	**+238**	+43	−10 285	−9 867	+461
Gained	282	**315**	285	291	115	255	475
Lost	**45**	233	47	248	10 400	10 122	14
vs. Theoretical Best (solves 32 633)							
Gained	83	80	85	**86**	32	76	**125**

180 s timeout, 38 717 benchmarks, unsat. only
ALIA, AUFLIA, AUFLIRA, UF, UFIDL, UFLIA, UFLRA

N is Normal, **E** is Eager, **S** is Solitary Variable, **d** is Deletion

Experimental Results: Baseline Strategies

vs. Default (solves 31 690)	N	E	S	Nd	Ed	Sd	Total
Solved	31 927	31 772	31 928	31 733	21 405	21 823	32 151
	+237	+82	**+238**	+43	−10 285	−9 867	+461
Gained	282	**315**	285	291	115	255	475
Lost	**45**	233	47	248	10 400	10 122	14
vs. Theoretical Best (solves 32 633)							
Gained	83	80	85	**86**	32	76	**125**

180 s timeout, 38 717 benchmarks, unsat. only
ALIA, AUFLIA, AUFLIRA, UF, UFIDL, UFLIA, UFLRA

N is Normal, **E** is Eager, **S** is Solitary Variable, **d** is Deletion

Experimental Results: Baseline Strategies

vs. Default (solves 31 690)	N	E	S	Nd	Ed	Sd	Total
Solved	31 927	31 772	31 928	31 733	21 405	21 823	32 151
	+237	+82	**+238**	+43	−10 285	−9 867	+461
Gained	282	**315**	285	291	115	255	475
Lost	**45**	233	47	248	10 400	10 122	14
vs. Theoretical Best (solves 32 633)							
Gained	83	80	85	**86**	32	76	**125**

180 s timeout, 38 717 benchmarks, unsat. only
ALIA, AUFLIA, AUFLIRA, UF, UFIDL, UFLIA, UFLRA

N is Normal, **E** is Eager, **S** is Solitary Variable, **d** is Deletion

Experimental Results: Baseline Strategies

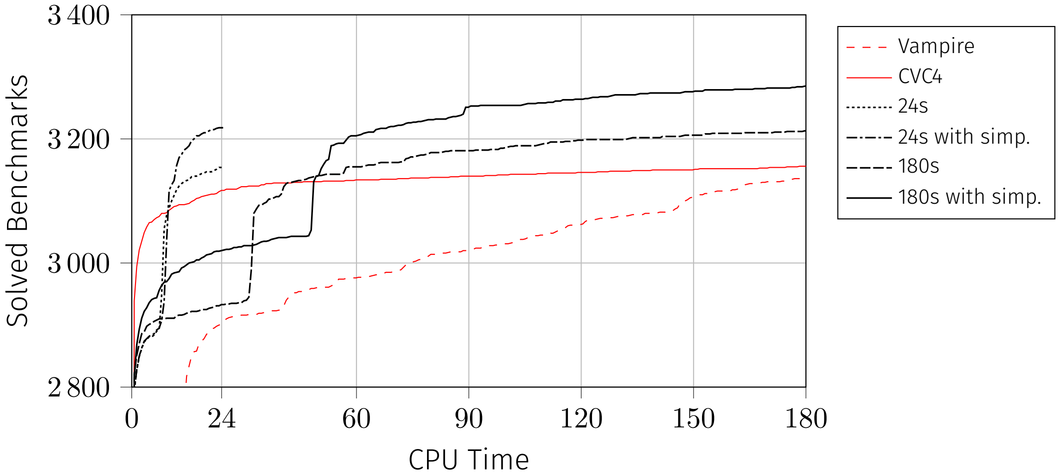
vs. Default (solves 31 690)	N	E	S	Nd	Ed	Sd	Total
Solved	31 927	31 772	31 928	31 733	21 405	21 823	32 151
	+237	+82	**+238**	+43	−10 285	−9 867	+461
Gained	282	**315**	285	291	115	255	475
Lost	**45**	233	47	248	10 400	10 122	14

vs. Theoretical Best (solves 32 633)	N	E	S	Nd	Ed	Sd	Total
Gained	83	80	85	**86**	32	76	125

180 s timeout, 38 717 benchmarks, unsat. only
ALIA, AUFLIA, AUFLIRA, UF, UFIDL, UFLIA, UFLRA

N is Normal, **E** is Eager, **S** is Solitary Variable, **d** is Deletion

Experimental Results: Schedules (UF only)



Thank you for Your Attention!