

Translation of Proofs Provided by External Provers

Mathias Fleury

ENS Rennes, Technische Universität München
May, 2nd – July, 31st
Jasmin Blanchette

September, 4th



1 Introduction

- Theorem proving
- Sledgehammer

2 Automatic solvers and Sledgehammer

3 Satallax

4 Conclusion

Interactive theorem prover trustful

- Kepler's conjecture (Hales, august 2014), Isabelle and HOL Light
- .seL4 microkernel (Klein, open sourcing in 2014), Isabelle

Automatic theorem prover tries to find proof as fast as possible. Not trustful.

- EQP (1998): proof of "Robbins conjecture"

Interactive theorem prover trustful

- Kepler's conjecture (Hales, august 2014), Isabelle and HOL Light
- .seL4 microkernel (Klein, open sourcing in 2014), Isabelle

Automatic theorem prover tries to find proof as fast as possible. Not trustful.

- EQP (1998): proof of “Robbins conjecture”

Sledgehammer

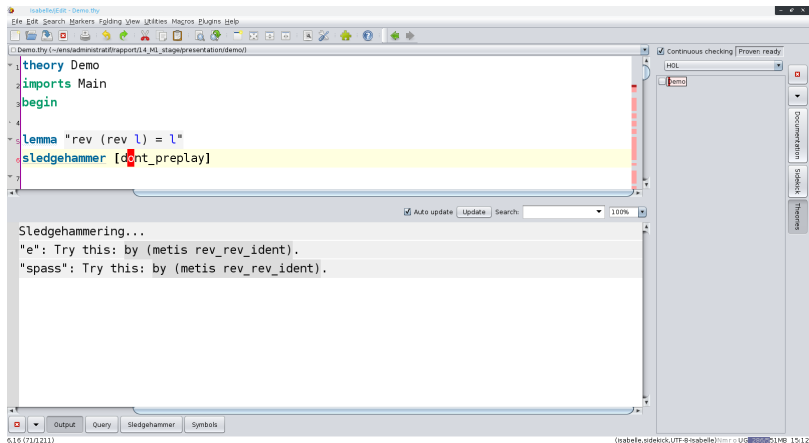


Figure: Sledgehammer finds lemmas

Sledgehammer

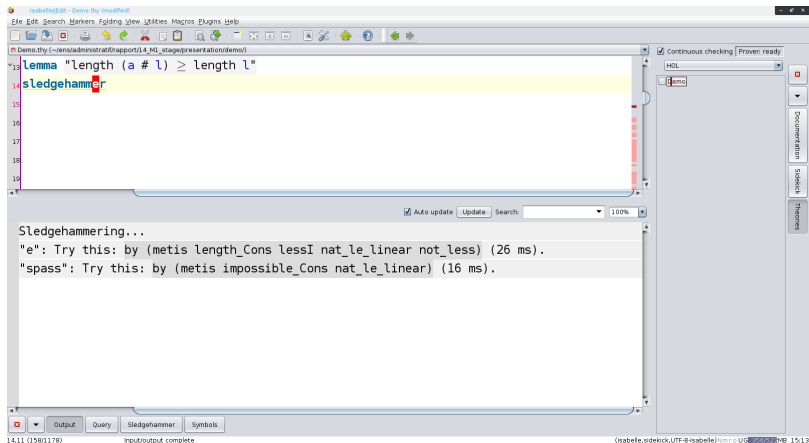


Figure: Sledgehammer finds also simple proofs

Sledgehammer

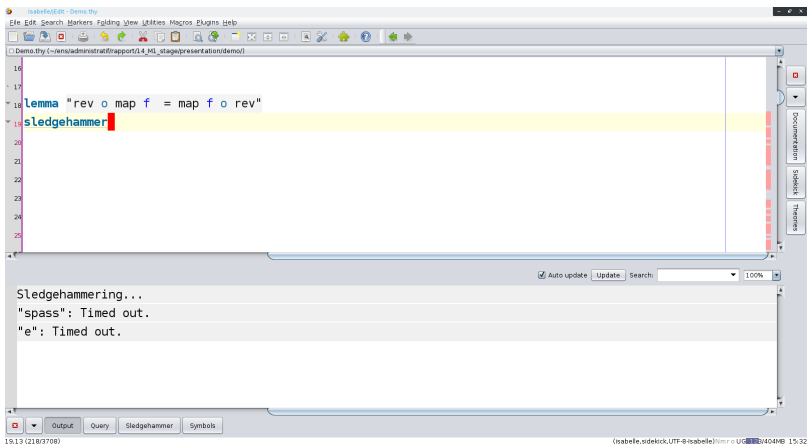
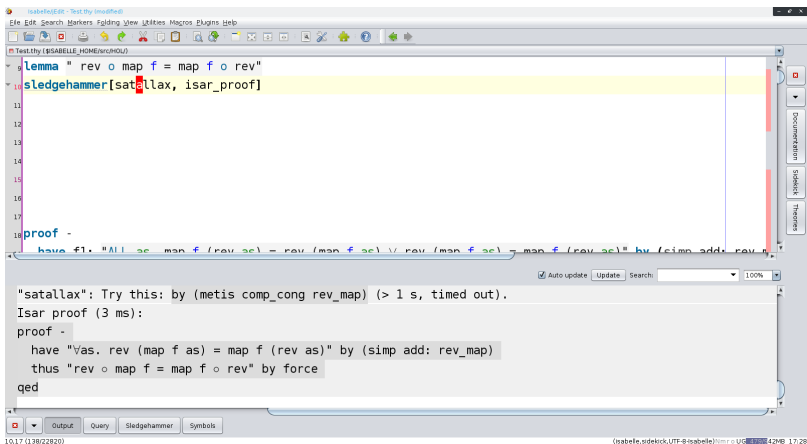


Figure: But is not as good for HO goals: no proof found

Sledgehammer



```

1  lemma " rev o map f = map f o rev "
2  sledgehammer[satallax, isar_proof]
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18 proof -
19   have f1: "All as. map f (rev as) = rev (map f as) ∨ rev (map f as) = map f (rev as)" by (simp add: rev_map)
20
21   "satallax": Try this: by (metis comp_cong rev_map) (> 1 s, timed out).
22   Isar proof (3 ms):
23   proof -
24     have "∀as. rev (map f as) = map f (rev as)" by (simp add: rev_map)
25     thus "rev o map f = map f o rev" by force
26   qed
  
```

10.17 (138/2820) (isabelle.sidekick.UTF-8@isabelle)sum o UC: 42MB 17.28

Figure: Calling a higher order prover

1 Introduction

2 Automatic solvers and Sledgehammer

- Two types of automatic solvers
- Sledgehammer

3 Satallax

4 Conclusion

Sledgehammer Call

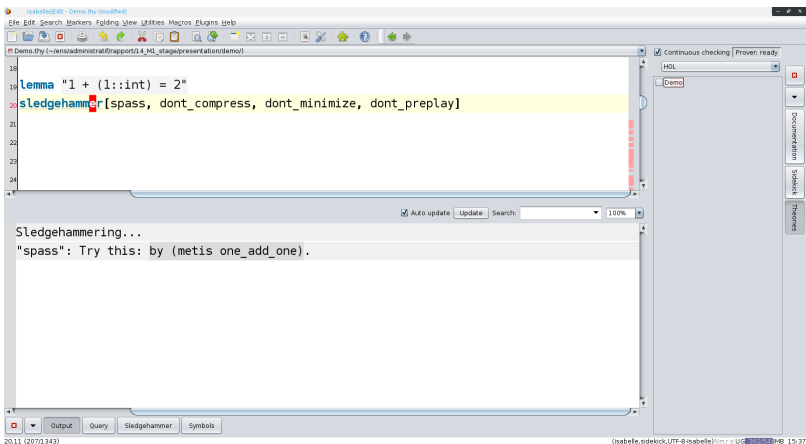


Figure: Automatic Theorem Provers (ATPs, historical sense): no arithmetic

Sledgehammer Call

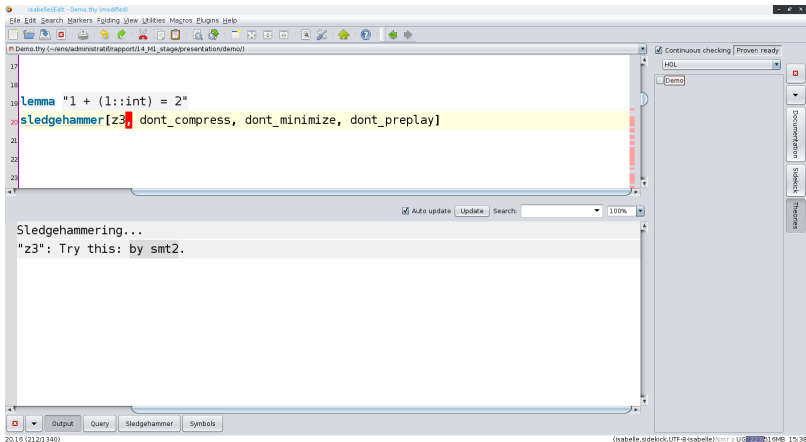


Figure: Satisfiability Modulo Theories solvers (SMT-solvers)

Sledgehammer

Fact filtering, ATP Translation

Fact filtering, SMT Translation

E

Leo-II

Satallax

veriT

Z3

CVC3



Figure: Sledgehammer organisation with reconstruction support with some of the supported provers (grey: done during the internship, upper half-circle means only fact-filtering, full half-circle means proof reconstruction)

- no trust in the prover
- no need to have it installed on the machine

1 Introduction

2 Automatic solvers and Sledgehammer

3 Satallax

- Backward and forward proofs
- Transformation
- Validation

4 Conclusion

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and

$B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

$[A; B]:$

$A \rightarrow 0 < S 0$

$[A; B; 0 < S 0]:$

$B \rightarrow 0 < S 0 \rightarrow$

$S 0 < S S 0$

$[A; B; 0 < 1; S 0 < S S 0]:$

$B \rightarrow S 0 <$

$S S 0 \rightarrow S S 0 <$

$S S S 0$

$[A; B; 0 < 1; S 0 < S 1; S S 0 < S S S 0]:$

$2 < 3$ is true.

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and

$B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

$[A; B]:$

$A \rightarrow 0 < S 0$

$[A; B; 0 < S 0]:$

$B \rightarrow 0 < S 0 \rightarrow$
 $S 0 < S S 0$

$[A; B; 0 < 1; S 0 < S S 0]:$

$B \rightarrow S 0 <$
 $S S 0 \rightarrow S S 0 <$
 $S S S 0$

$[A; B; 0 < 1; S 0 < S 1; S S 0 < S S S 0]:$

$2 < 3$ is true.

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and

$B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

$[A; B]:$

$A \rightarrow 0 < S 0$

$[A; B; 0 < S 0]:$

$B \rightarrow 0 < S 0 \rightarrow$
 $S 0 < S S 0$

$[A; B; 0 < 1; S 0 < S S 0]:$

$B \rightarrow S 0 <$
 $S S 0 \rightarrow S S 0 <$
 $S S S 0$

$[A; B; 0 < 1; S 0 < S 1; S S 0 < S S S 0]:$

$2 < 3$ is true.

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and

$B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

$[A; B]:$

$A \rightarrow 0 < S 0$

$[A; B; 0 < S 0]:$

$B \rightarrow 0 < S 0 \rightarrow$
 $S 0 < S S 0$

$[A; B; 0 < 1; S 0 < S S 0]:$

$B \rightarrow S 0 <$
 $S S 0 \rightarrow S S 0 <$
 $S S S 0$

$[A; B; 0 < 1; S 0 < S 1; S S 0 < S S S 0]:$

$2 < 3$ is true.

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and

$B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

$[A; B]:$

$A \rightarrow 0 < S 0$

$[A; B; 0 < S 0]:$

$B \rightarrow 0 < S 0 \rightarrow$
 $S 0 < S S 0$

$[A; B; 0 < 1; S 0 < S S 0]:$

$B \rightarrow S 0 <$
 $S S 0 \rightarrow S S 0 <$
 $S S S 0$

$[A; B; 0 < 1; S 0 < S 1; S S 0 < S S S 0]:$

$2 < 3$ is true.

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and

$B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

$[A; B]:$

$A \rightarrow 0 < S 0$

$[A; B; 0 < S 0]:$

$B \rightarrow 0 < S 0 \rightarrow$

$S 0 < S S 0$

$[A; B; 0 < 1; S 0 < S S 0]:$

$B \rightarrow S 0 <$

$S S 0 \rightarrow S S 0 <$

$S S S 0$

$[A; B; 0 < 1; S 0 < S 1; S S 0 < S S S 0]:$

$2 < 3$ is true.

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and
 $B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

$[A; B]:$

$A \rightarrow 0 < S 0$

$[A; B; 0 < S 0]:$

$B \rightarrow 0 < S 0 \rightarrow$
 $S 0 < S S 0$

$[A; B; 0 < 1; S 0 < S S 0]:$

$B \rightarrow S 0 <$
 $S S 0 \rightarrow S S 0 <$
 $S S S 0$

$[A; B; 0 < 1; S 0 < S 1; S S 0 < S S S 0]:$

$2 < 3$ is true.

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and
 $B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

from assumption to conclusion

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and
 $B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

from assumption to conclusion

Backward proof

3	$\frac{A, B}{S 0 < S S 0}$	$B \rightarrow 0 < S 0 \rightarrow S 0 < S S 0$, new goals : 4 and 5
4	$\frac{A, B}{B}$	B
5	$\frac{A, B}{0 < S 0}$	is true thanks to A

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and
 $B := \forall(m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

from assumption to conclusion

Backward proof

3	$\frac{A, B}{S 0 < S S 0}$	$B \rightarrow 0 < S 0 \rightarrow S 0 < S S 0$, new goals : 4 and 5
4	$\frac{A, B}{B}$	B
5	$\frac{A, B}{0 < S 0}$	is true thanks to A

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and
 $B := \forall(m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

from assumption to conclusion

Backward proof

3	$\frac{A, B}{S 0 < S S 0}$	$B \rightarrow 0 < S 0 \rightarrow S 0 < S S 0$, new goals : 4 and 5
4	$\frac{A, B}{B}$	B
5	$\frac{A, B}{0 < S 0}$	is true thanks to A

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and
 $B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

from assumption to conclusion

Backward proof

3	$\frac{A, B}{S 0 < S S 0}$	$B \rightarrow 0 < S 0 \rightarrow S 0 < S S 0$, new goals : 4 and 5
4	$\frac{A, B}{B}$	B
5	$\frac{A, B}{0 < S 0}$	is true thanks to A

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and
 $B := \forall(m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

from assumption to conclusion

Backward proof

3	$\frac{A, B}{S 0 < S S 0}$	$B \rightarrow 0 < S 0 \rightarrow S 0 < S S 0$, new goals : 4 and 5
4	$\frac{A, B}{B}$	B
5	$\frac{A, B}{0 < S 0}$	is true thanks to A

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and
 $B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

from assumption to conclusion

Backward proof

3	$\frac{A, B}{S0 < SS0}$	$B \rightarrow 0 < S0 \rightarrow S0 < SS0$, new goals : 4 and 5
4	$\frac{A, B}{B}$	B
5	$\frac{A, B}{0 < S0}$	is true thanks to A

Define $<$ as : $A := \forall n \in \mathbb{N}, 0 < S n$ and
 $B := \forall (m, n) \in \mathbb{N}, m < n \rightarrow S m < S n$. Show that $2 < 3$.

Forward proof

from assumption to conclusion

Backward proof

From conclusion to assumption

Proof representation

Assuming $\neg R, P \vee Q, \neg Q \vee R$, have $P \wedge \neg R$.

Proof representation

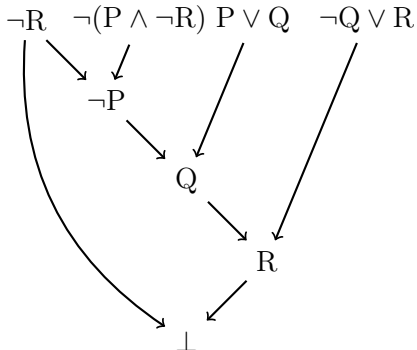


Figure: Forward proof representation example.

$$\text{a2: } \neg Q \vee R \quad \frac{\text{h0: } \neg(P \wedge \neg R)}{\text{1: } \perp} \quad \text{Satallax}$$

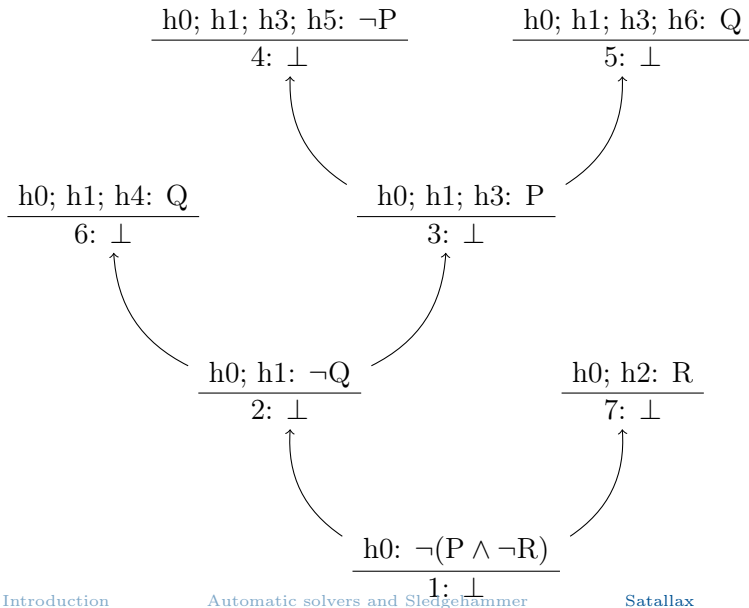
$$(\neg(A \wedge B)) \rightarrow (\neg A \rightarrow \perp) \rightarrow (\neg B \rightarrow \perp) \rightarrow (\neg(A \wedge B) \rightarrow \perp)$$

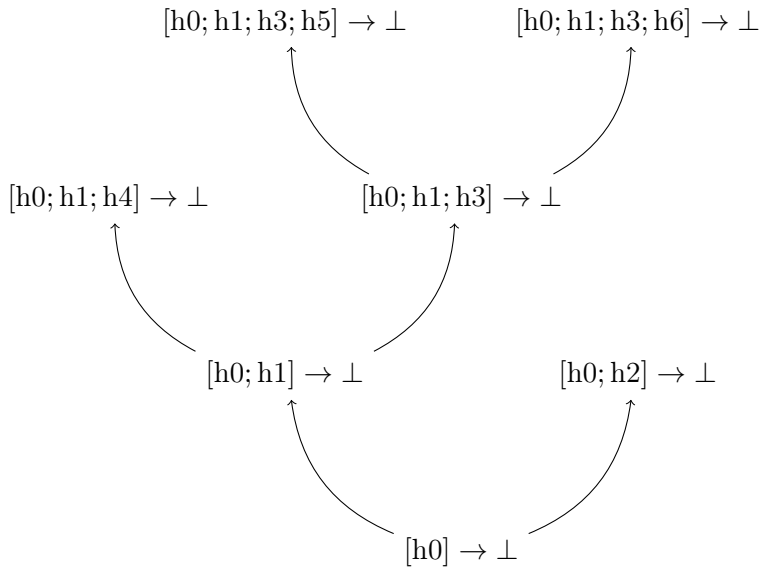
$$\begin{array}{ccc}
 a3: P \vee Q \frac{h0; h1: \neg Q}{2: \perp} & & a1 : \neg R \frac{h0; h2: R}{7: \perp} a1, h2 \\
 \uparrow (i) & & \uparrow (i) \\
 a2: \neg Q \vee R \frac{h0: \neg(P \wedge \neg R)}{1: \perp} & \text{Satallax} &
 \end{array}$$

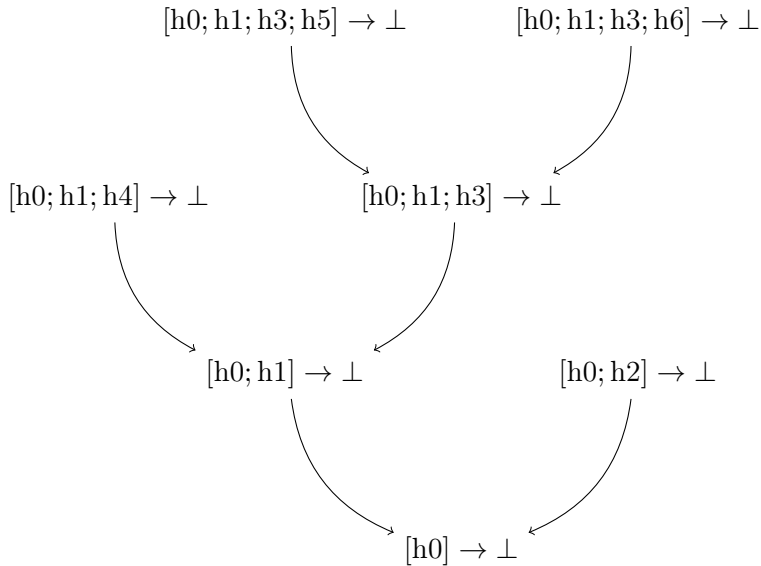
$$(A \vee B) \rightarrow (A \rightarrow \perp) \rightarrow (B \rightarrow \perp) \rightarrow ((A \vee B) \rightarrow \perp)$$

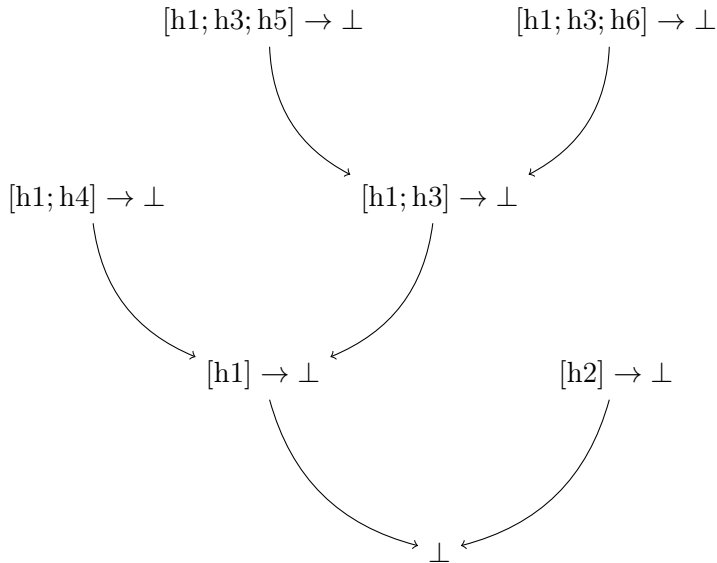
$$\begin{array}{ccc}
 \frac{h0; h1; h4: Q}{6: \perp} \quad h4, h1 & & h0 \quad \frac{h0; h1; h3: P}{3: \perp} \\
 \uparrow (i) & & \uparrow (i) \\
 a3: P \vee Q \quad \frac{h0; h1: \neg Q}{2: \perp}
 \end{array}$$

$$\begin{array}{c}
 \frac{h0; h1; h3; h5: \neg P}{4: \perp} \quad h3, h5 \quad \frac{h0; h1; h3; h6: Q}{5: \perp} \quad a1: \neg R, h6 \\
 \qquad \qquad \qquad \uparrow \qquad \qquad \qquad \uparrow \\
 \text{(ii)} \qquad \qquad \qquad \text{(ii)} \\
 \frac{h0; h1; h4: Q}{6: \perp} \quad h4, h1 \qquad h0 \quad \frac{h0; h1; h3: P}{3: \perp}
 \end{array}$$









Validation

- Tests using Mirabelle (tools that test every step);
- No documentation, so test necessary (many surprises!);
- No description of the rules

- 1 Introduction
- 2 Automatic solvers and Sledgehammer
- 3 Satallax
- 4 Conclusion**

- 4 new provers (Leo-II, Satallax, Zipperposition, veriT) added:
 - Leo-II and Satallax should improve overall performance (with HO goals)
 - Zipperposition is another ATP
 - veriT is the second SMT-solver (with arithmetics!)
- Allows developers to optimize for goals produced by humans

Questions?

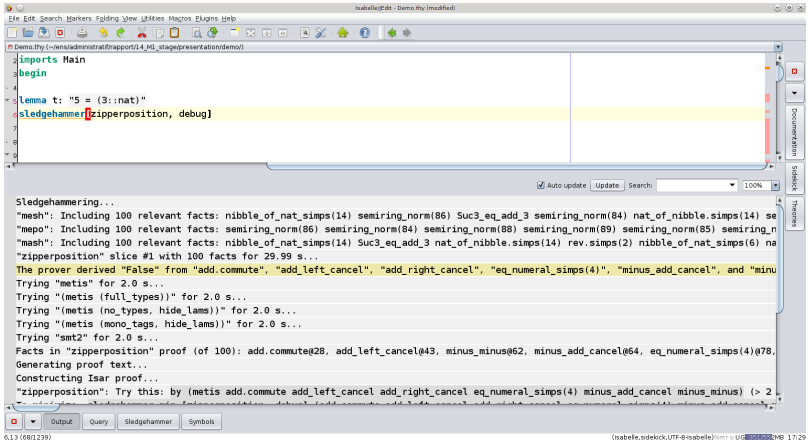


Figure: XKCD 1403

5 Annex

- Trust

Isabelle



The screenshot shows the Isabelle IDE interface. The top pane displays a proof script in a file named `demo.thy`. The script includes the following code:

```

imports Main
begin
lemma t: "5 = (3::nat)"
sledgehammer[zipperposition, debug]

```

The bottom pane shows the output of the `sledgehammer` command. It reports that the prover derived a "False" result from various tactics, including `add_commute`, `add_left_cancel`, `add_right_cancel`, `eq_numeral_simps(4)`, `minus_add_cancel`, and `minus_minus`. It then lists several tactics it tried for 2.0 seconds, such as `metis`, `metis (full_types)`, `metis (no_types, hide_lams)`, `metis (mono_tags, hide_lams)`, and `smt2`. The output concludes with the text: "Facts in 'zipperposition' proof (of 100): add.commute@28, add_left_cancel@43, minus_minus@62, minus_add_cancel@64, eq_numeral_simps(4)@78. Generating proof text... Constructing Isar proof... 'zipperposition': Try this: by (metis add.commute add_left_cancel add_right_cancel eq_numeral_simps(4) minus_add_cancel minus_minus) (> 2.0 s)".

Figure: Isabelle call to Zipperposition through Sledgehammer

Isabelle

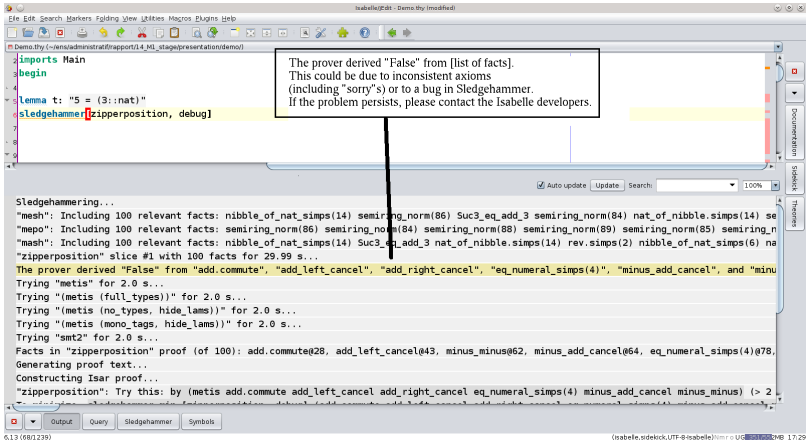
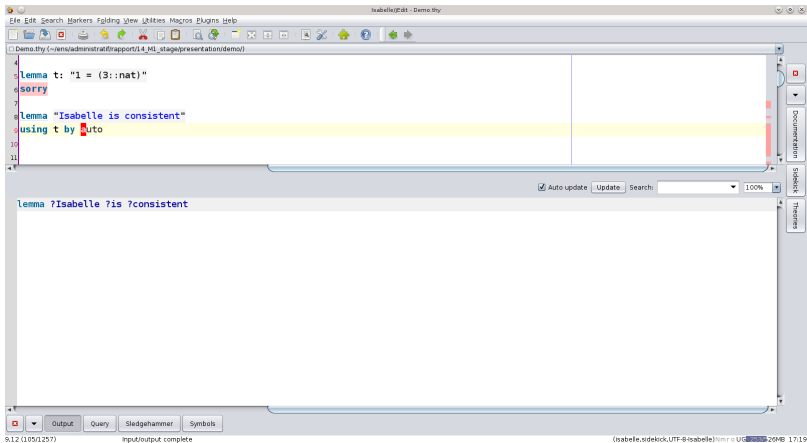


Figure: Isabelle call to Zipperposition through Sledgehammer

Annex

Bugs?



The screenshot shows the Isabelle/IDE interface. The main editor contains the following code:

```

4 lemma t: "1 = (3::nat)"
5 sorry
7 lemma "Isabelle is consistent"
8 using t by auto
10
11
  
```

The line `using t by auto` is highlighted in yellow. Below the editor, the command prompt shows the command `lemma ?Isabelle ?is ?consistent`. The status bar at the bottom indicates `input/output complete` and `9.12 (1050257)`. The right sidebar shows the `sidekick` panel with `Documentation`, `sidekick`, and `Theories` tabs.

Figure: Isabelle is inconsistent

Bugs?

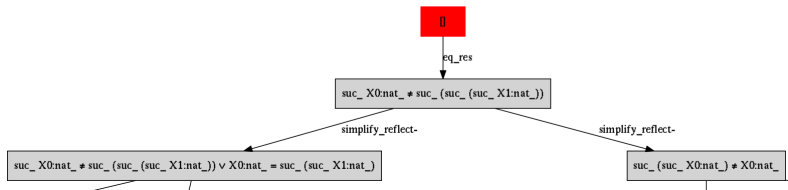


Figure: Zipperposition bug: $\forall X0, X1, X0 + 1 \neq X1 + 3$, from a consistent set of axioms (Isabelle's nat). It has been corrected.

Annex