Translation of Proofs Provided by External Provers

Mathias Fleury

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

September, 4th

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

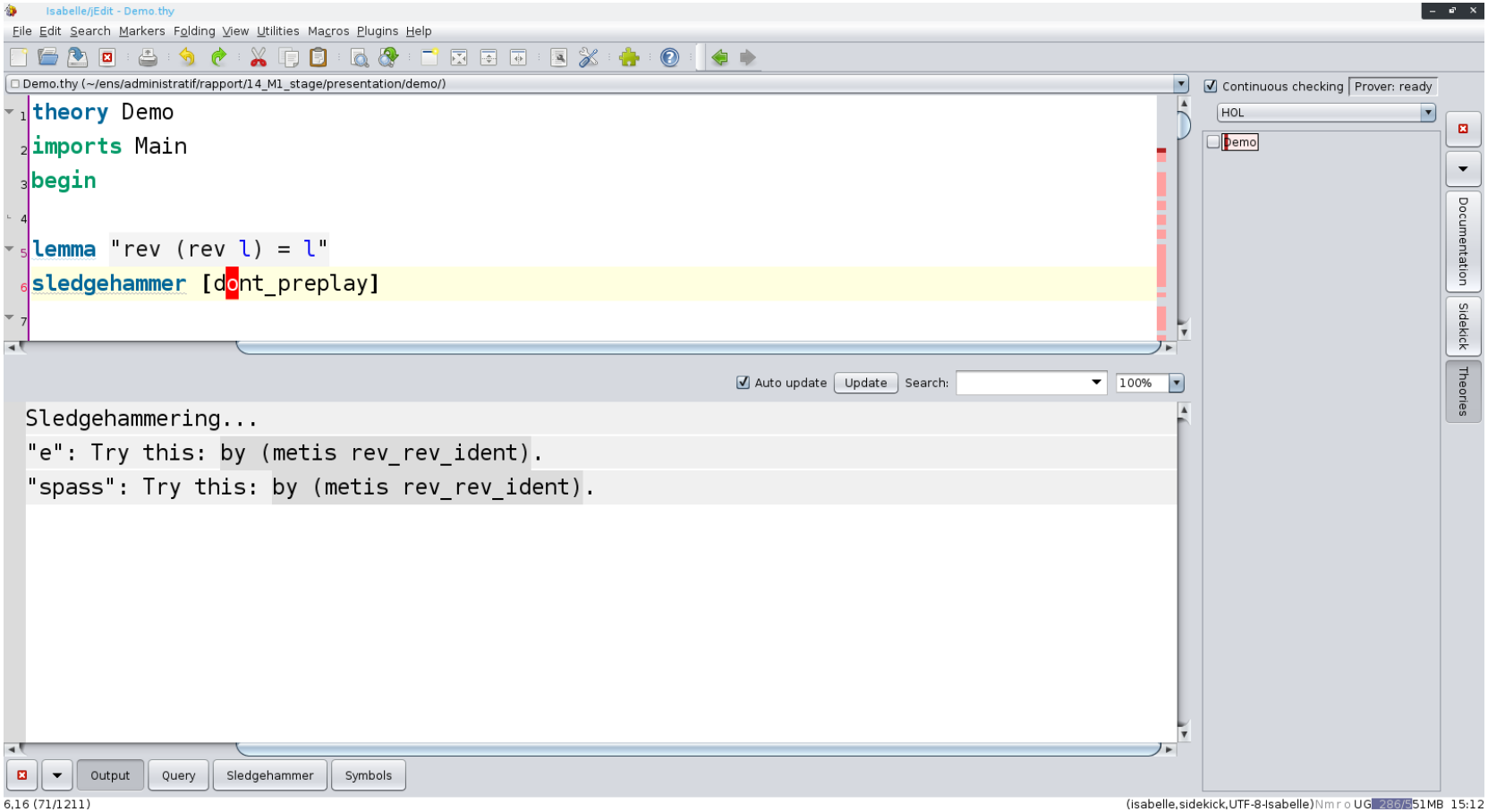


Figure: Sledgehammer finds lemmas

Sledgehammer

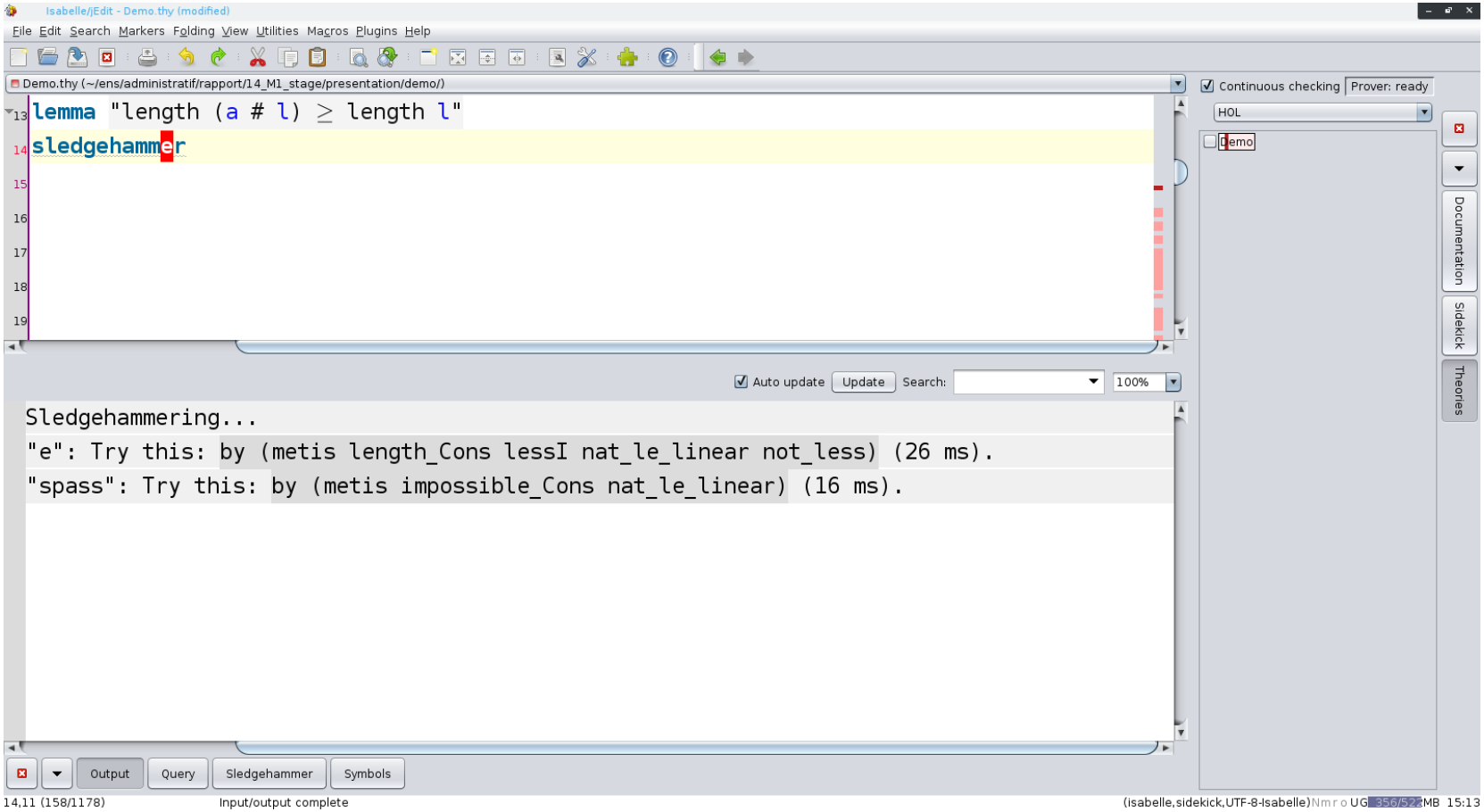


Figure: Sledgehammer finds also simple proofs

Sledgehammer

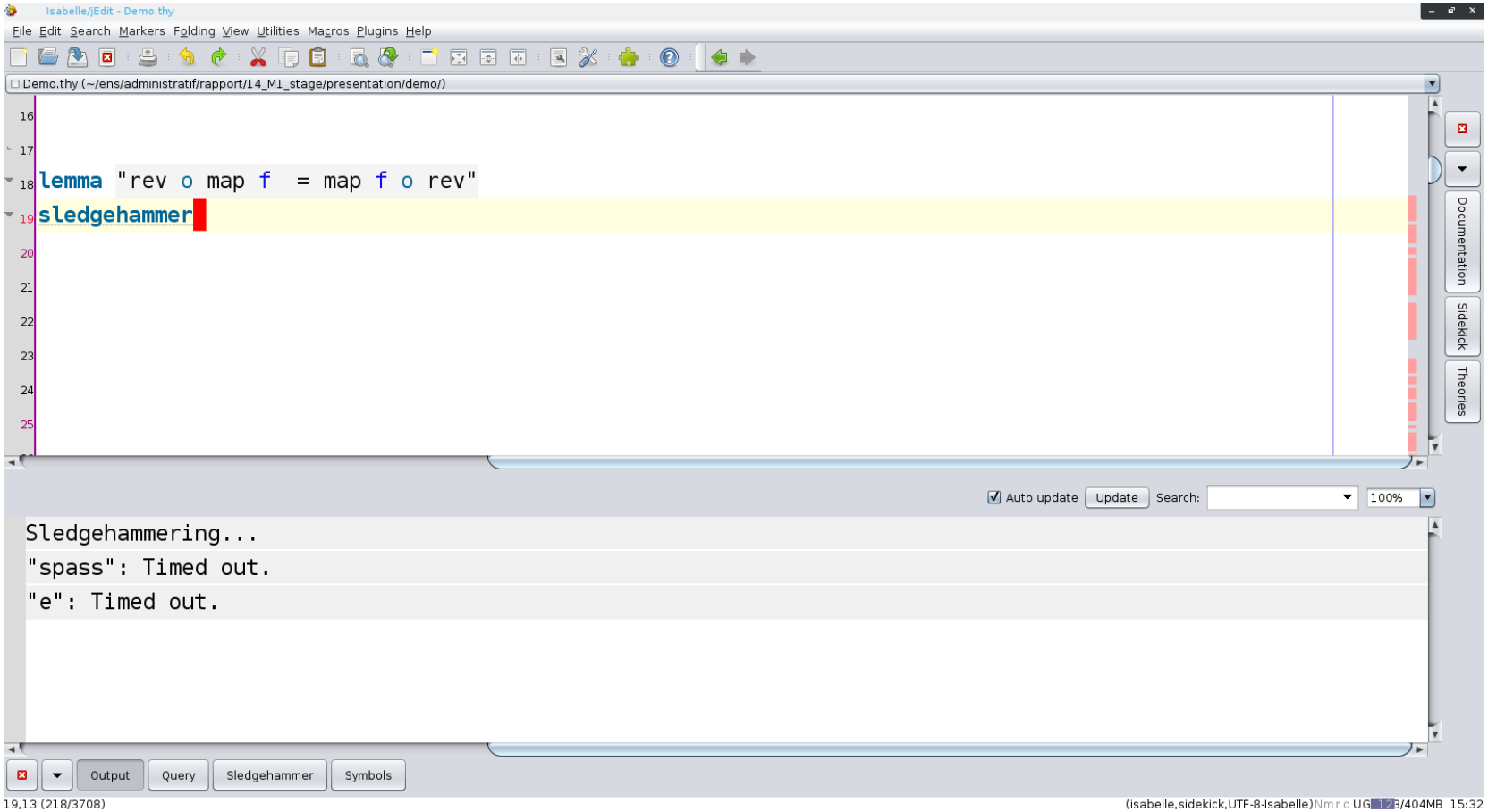


Figure: But is not as good for HO goals: no proof found

Sledgehammer

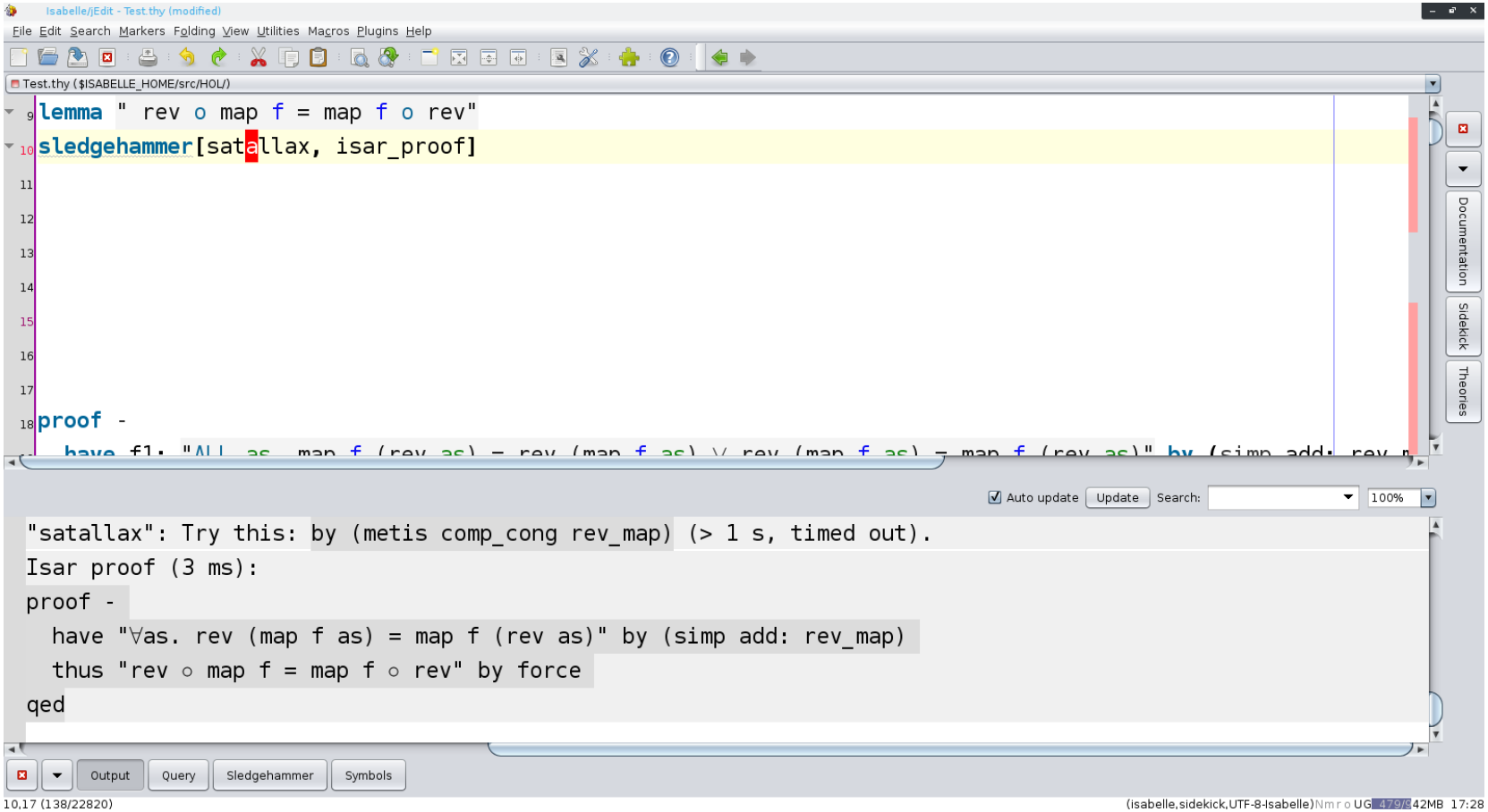


Figure: Calling a higher order prover

Sledgehammer Call

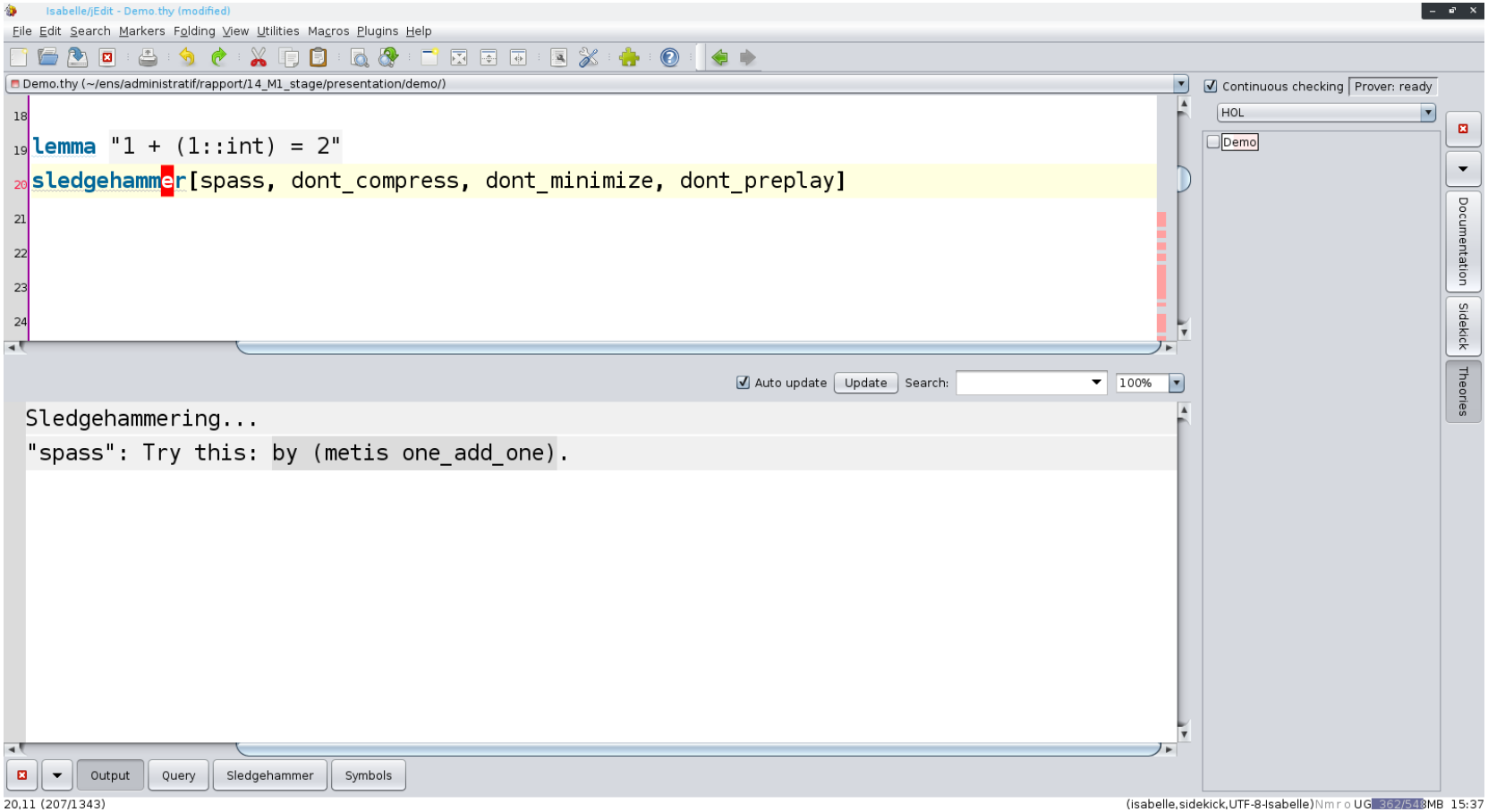


Figure: Automatic Theorem Provers (ATPs, historical sense): no arithmetic

Sledgehammer Call

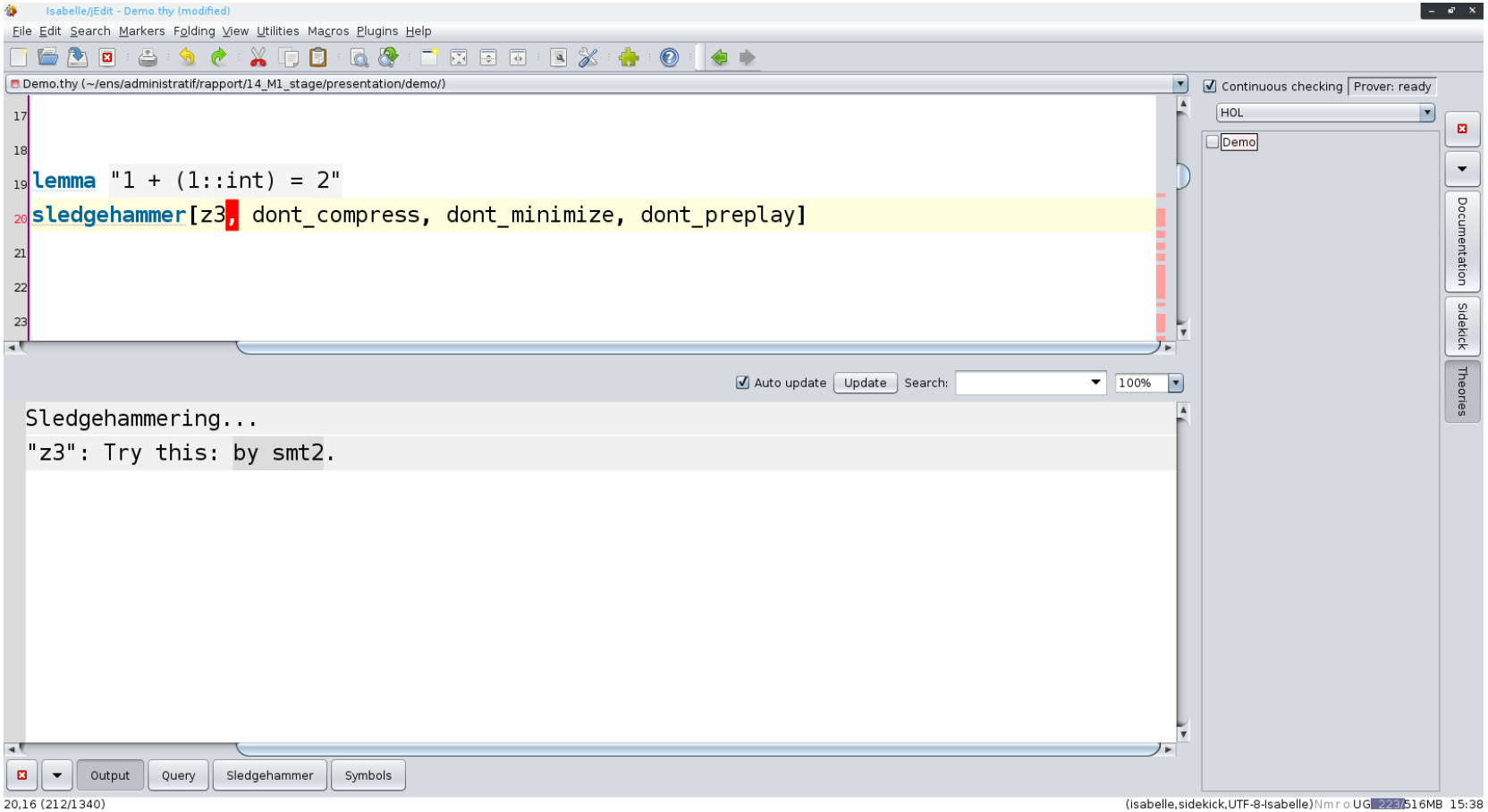


Figure: Satisfiability Modulo Theories solvers (SMT-solvers)

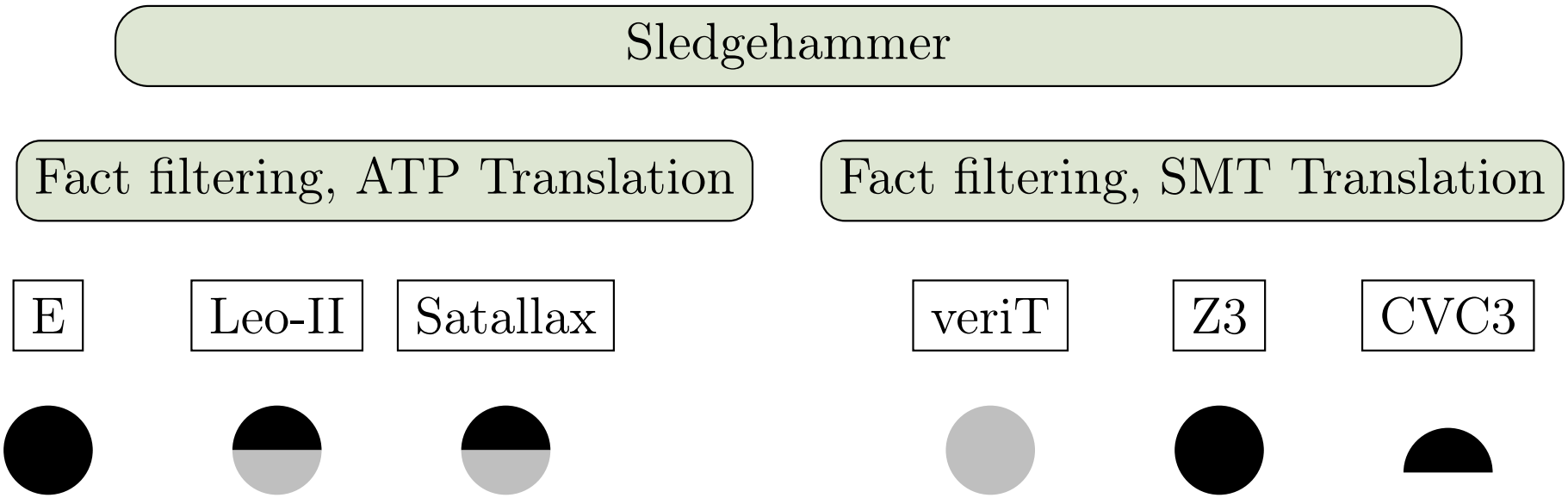


Figure: Sledgehammer organisation with reconstruction support with some of the supported provers (grey: done during the internship, upper half-circle means only fact-filtering, full half-circle means proof reconstruction)

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

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

Forward proof

$[A; B]$:

$A \to 0 < S\,0$

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

$B \to 0 < S\,0 \to S\,0 < S\,S\,0$

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

$B \to S\,0 < S\,S\,0 \to S\,S\,0 < S\,S\,S\,0$

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

$2 < 3$ is true.

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

Forward proof

$[A; B]$:

$A \to 0 < S\,0$

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

$B \to 0 < S\,0 \to S\,0 < S\,S\,0$

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

$B \to S\,0 < S\,S\,0 \to S\,S\,0 < S\,S\,S\,0$

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

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

Forward proof

$[A; B]$:

$A \to 0 < S\,0$

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

$B \to 0 < S\,0 \to S\,0 < S\,S\,0$

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

$B \to S\,0 < S\,S\,0 \to S\,S\,0 < S\,S\,S\,0$

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

$2 < 3$ is true.

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

Forward proof

$[A; B]$:

$A \to 0 < S\,0$

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

$B \to 0 < S\,0 \to S\,0 < S\,S\,0$

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

$B \to S\,0 < S\,S\,0 \to S\,S\,0 < S\,S\,S\,0$

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

$2 < 3$ is true.

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

Forward proof

$[A; B]$:

$A \to 0 < S\,0$

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

$B \to 0 < S\,0 \to S\,0 < S\,S\,0$

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

$B \to S\,0 < S\,S\,0 \to S\,S\,0 < S\,S\,S\,0$

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

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

Forward proof

from assumption to conclusion

Backward proof

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

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

Forward proof

from assumption to conclusion

Backward proof

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

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

Forward proof

from assumption to conclusion

Backward proof

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

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

Forward proof

from assumption to conclusion

Backward proof

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

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

Forward proof

from assumption to conclusion

Backward proof

3	$\dfrac{A, B}{S\,0 < S\,S\,0}$	$B \to 0 < S\,0 \to S\,0 < S\,S\,0$, new goals : 4 and 5
4	$\dfrac{A, B}{B}$	B
5	$\dfrac{A, B}{0 < S\,0}$	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	$\dfrac{A, B}{S\,0 < S\,S\,0}$	$B \rightarrow 0 < S\,0 \rightarrow S\,0 < S\,S\,0$, new goals : 4 and 5
4	$\dfrac{A, B}{B}$	B
5	$\dfrac{A, B}{0 < S\,0}$	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

From conclusion to assumption

Proof representation

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

Proof representation

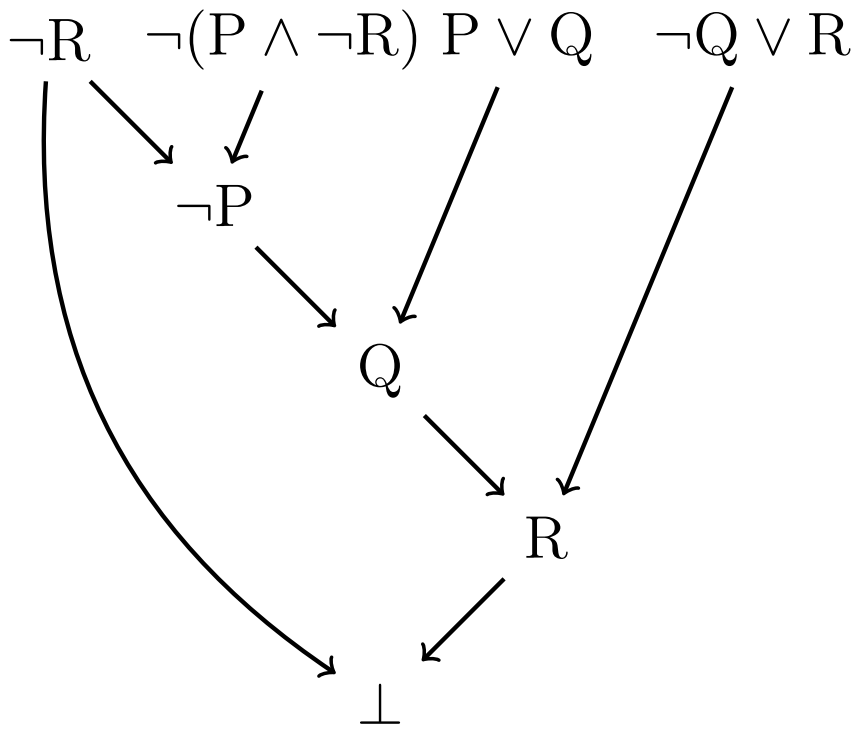
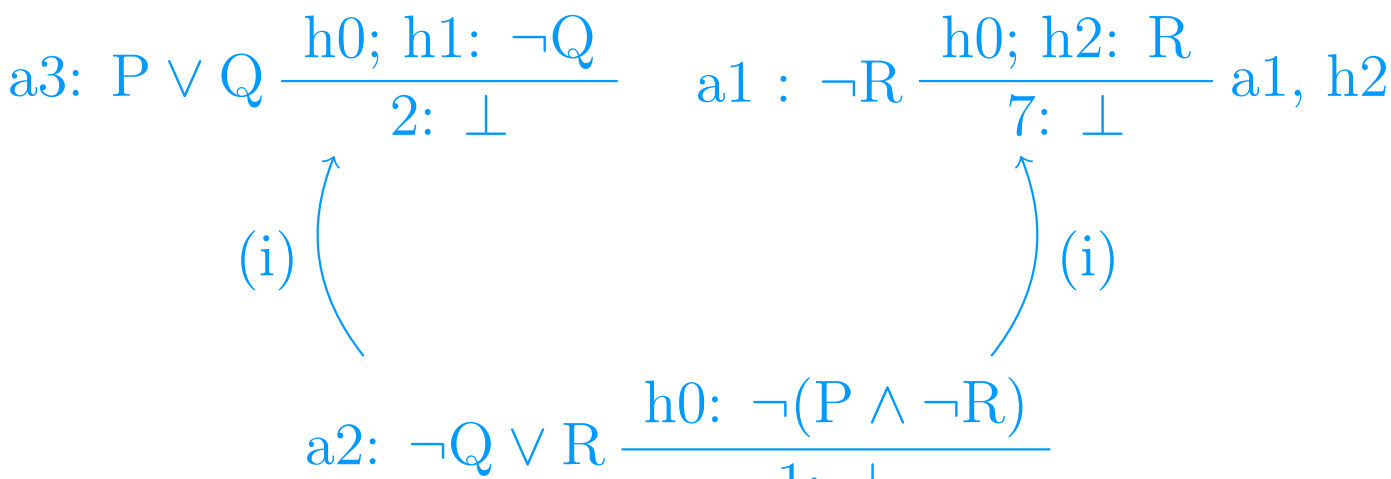


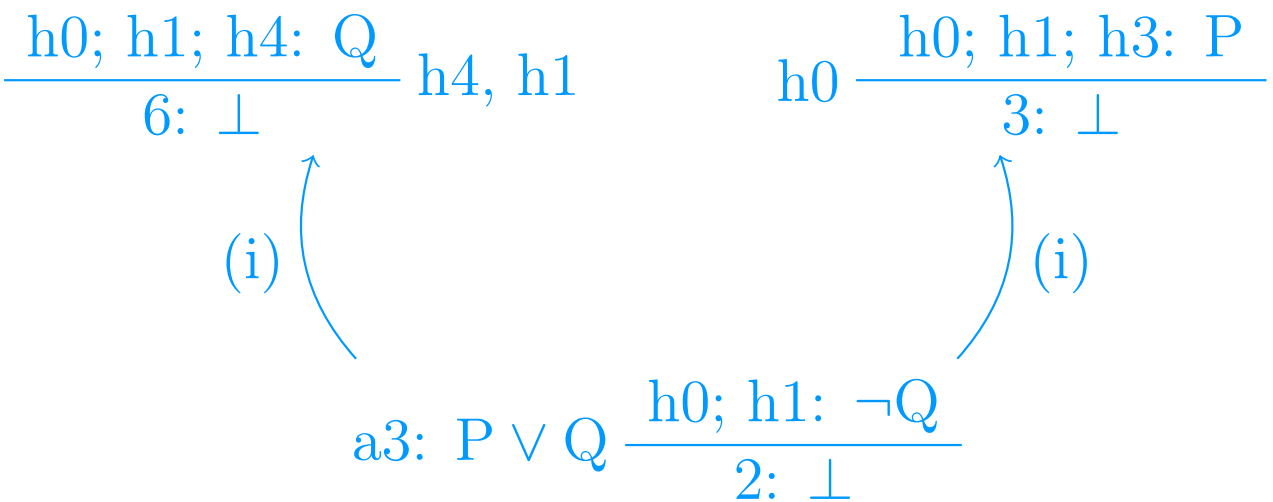
Figure: Forward proof representation example.

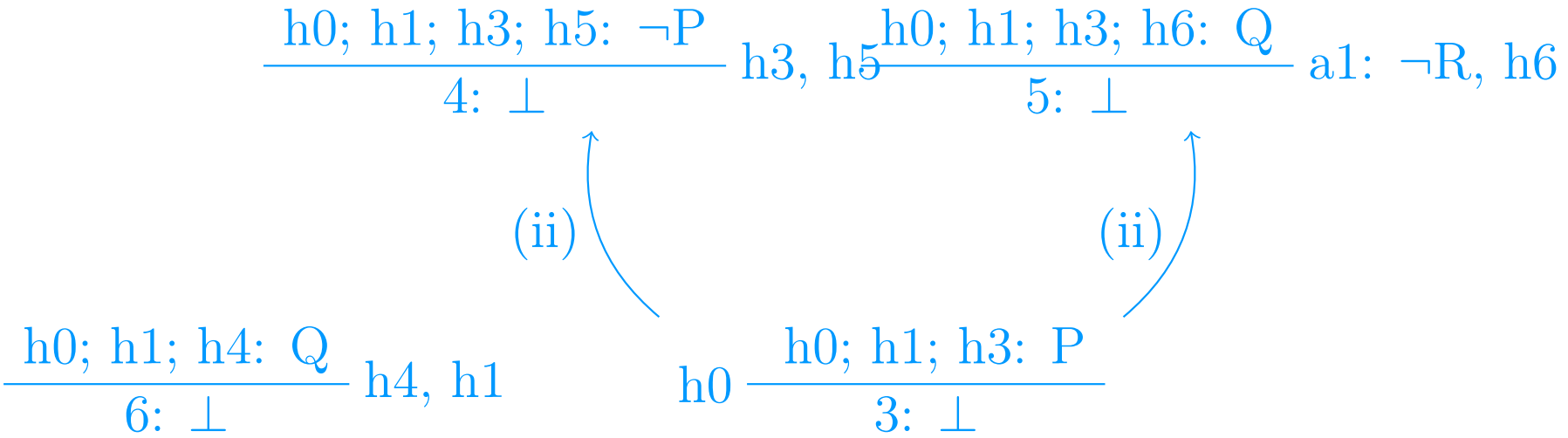
$$\text{a2: } \neg Q \vee R \quad \frac{\text{h0: } \neg(P \wedge \neg R)}{\text{1: } \bot}$$

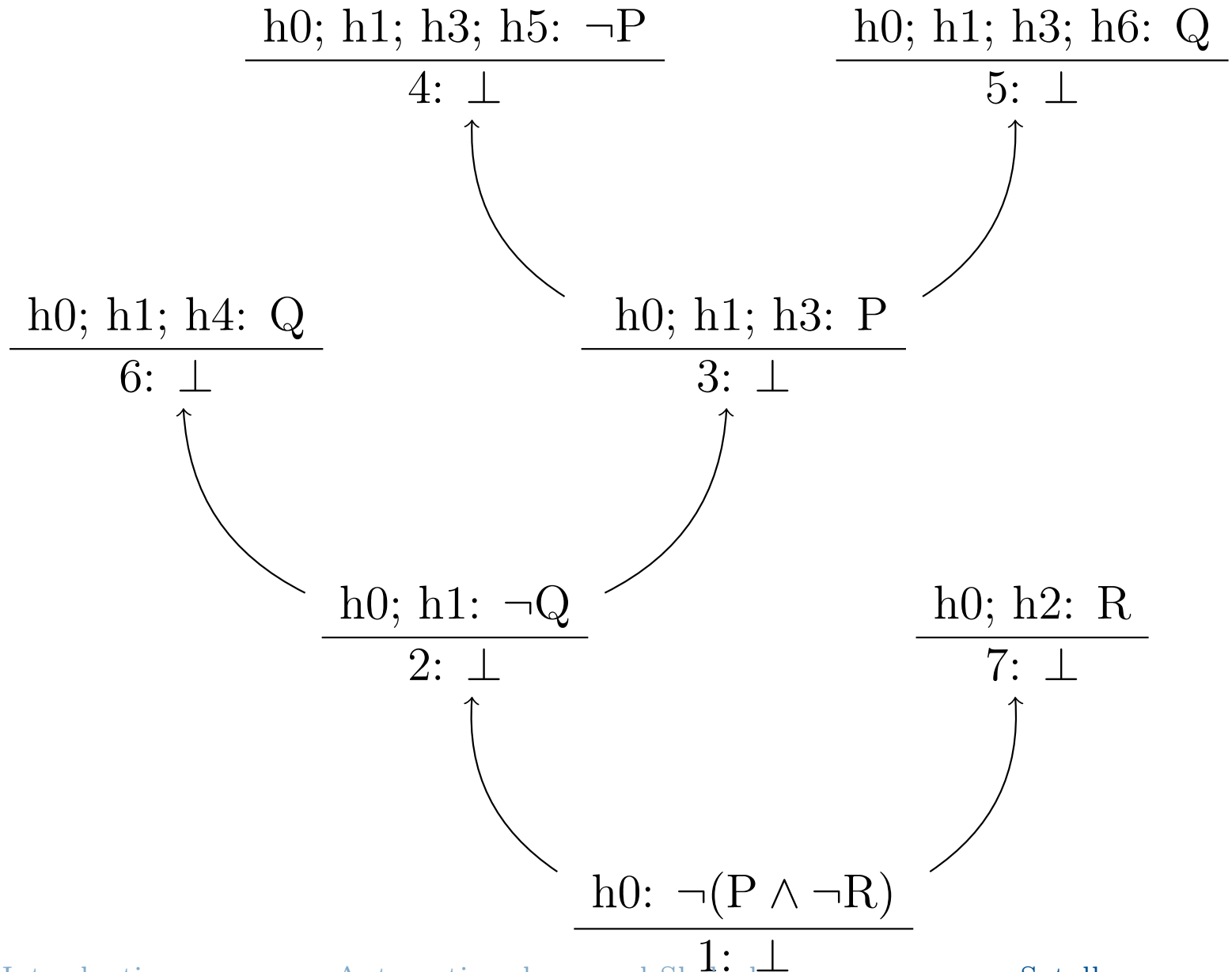
$$(\neg\,(\mathrm{A} \wedge \mathrm{B})) \to (\neg \mathrm{A} \to \bot) \to (\neg \mathrm{B} \to \bot) \to (\neg\,(\mathrm{A} \wedge \mathrm{B}) \to \bot)$$

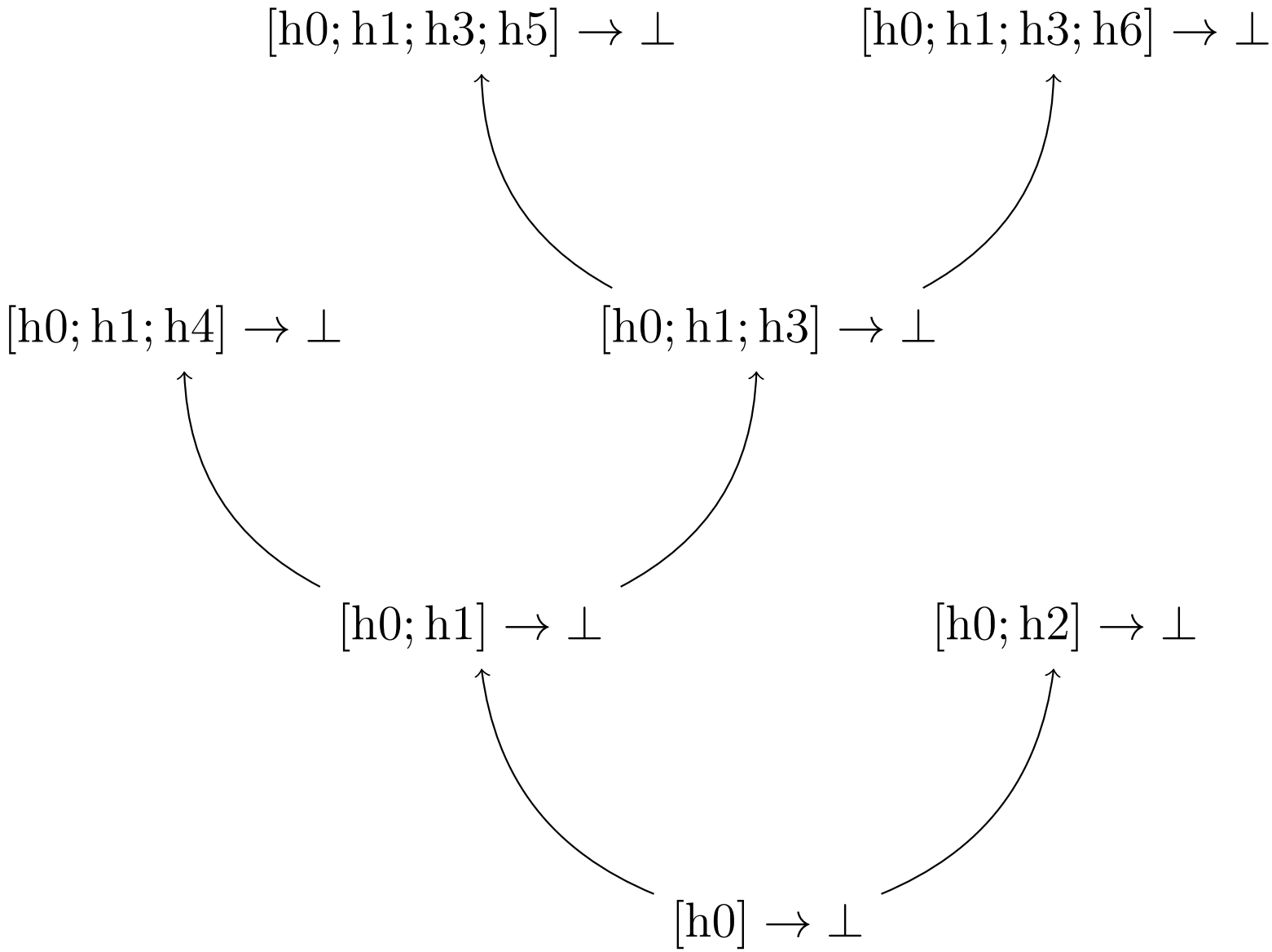

a3: P ∨ Q
h0; h1: ¬Q
2: ⊥
a1 : ¬R
h0; h2: R
7: ⊥
a1, h2
(i)
(i)
a2: ¬Q ∨ R
h0: ¬(P ∧ ¬R)
1: ⊥

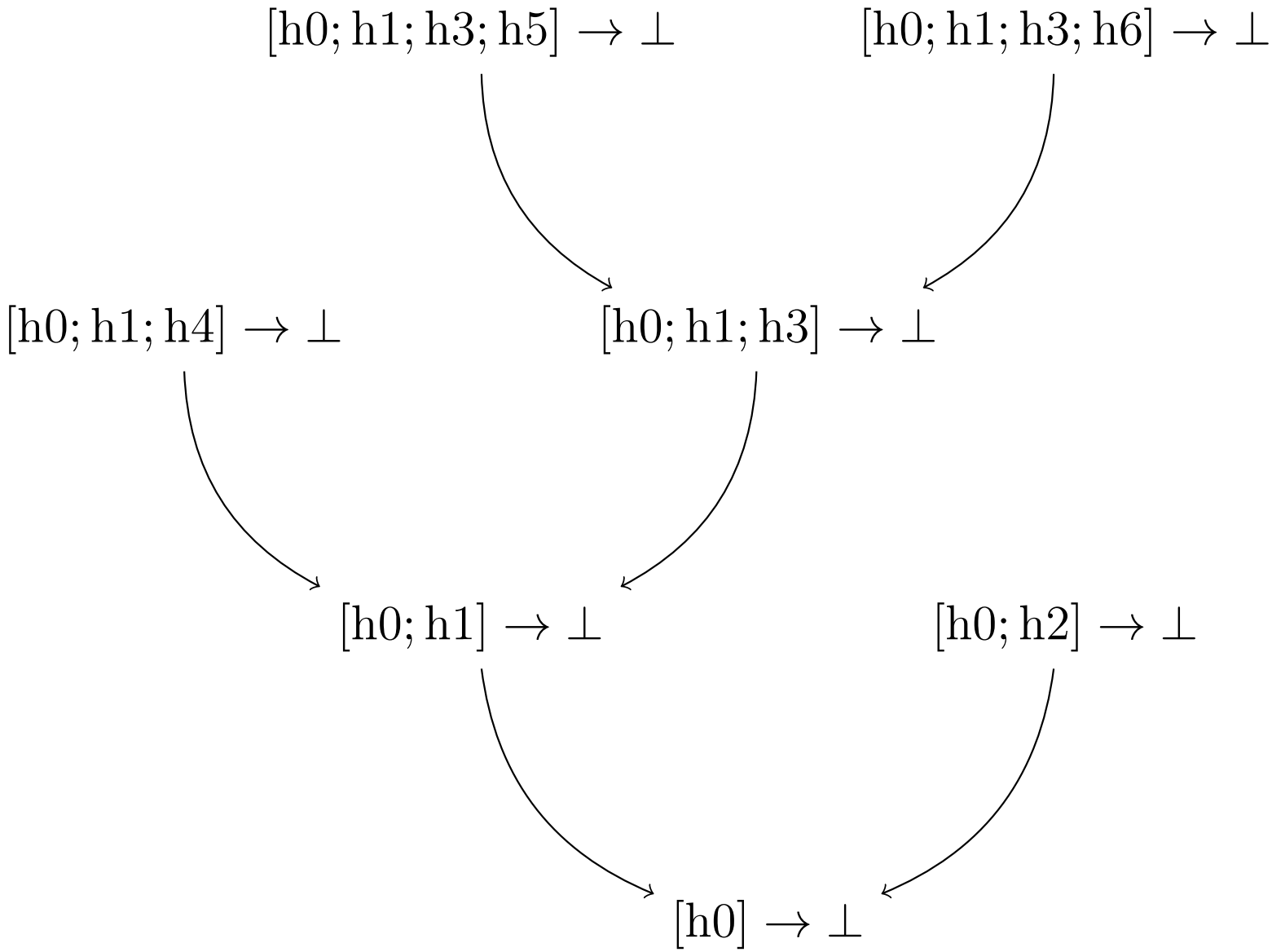
$$(A \vee B) \to (A \to \bot) \to (B \to \bot) \to ((A \vee B) \to \bot)$$

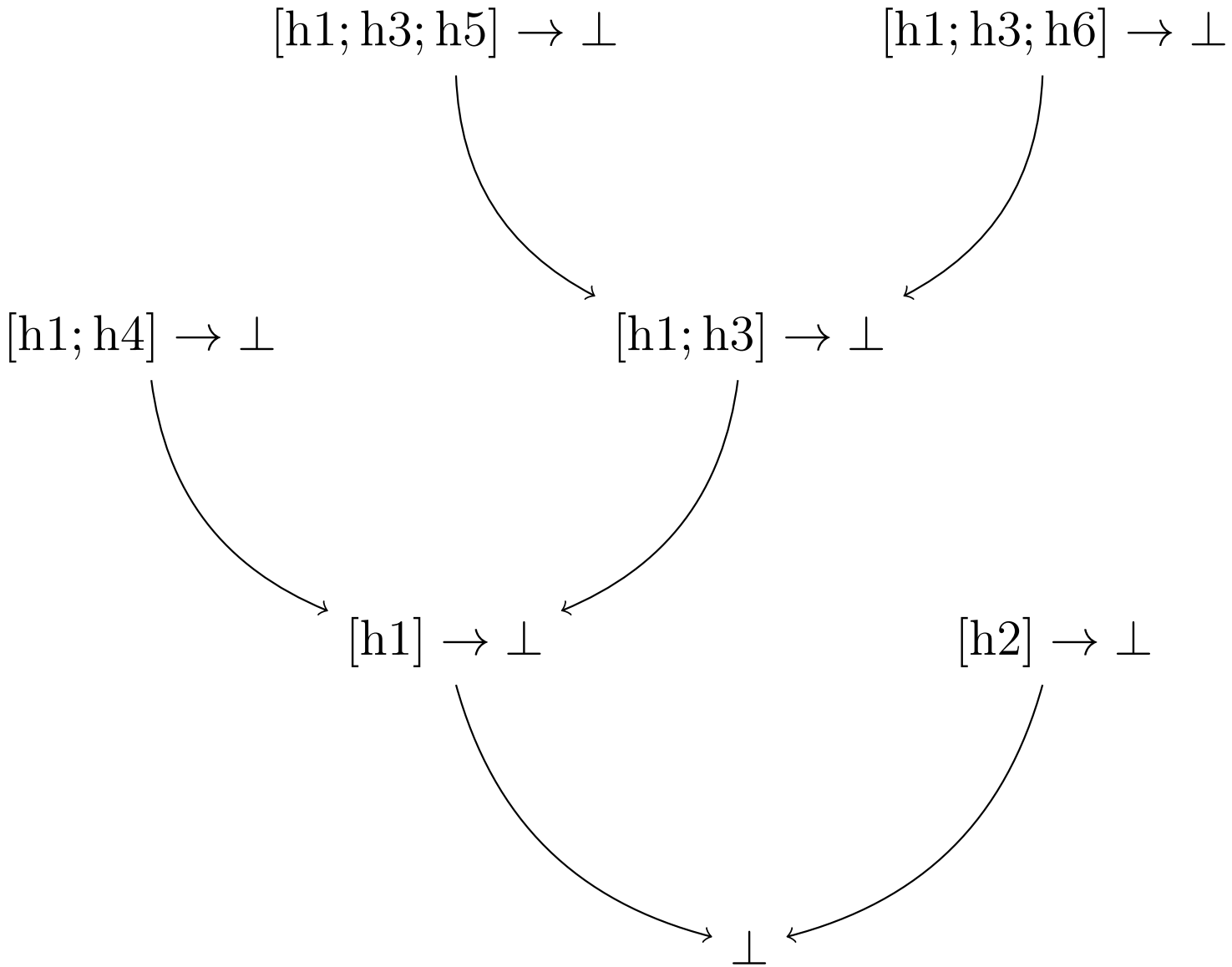

h0; h1; h4: Q
6: ⊥
h4, h1
h0
h0; h1; h3: P
3: ⊥
(i)
(i)
a3: P ∨ Q
h0; h1: ¬Q
2: ⊥


h0; h1; h3; h5: ¬P
4: ⊥
h3, h5
h0; h1; h3; h6: Q
5: ⊥
a1: ¬R, h6
(ii)
(ii)
h0; h1; h4: Q
6: ⊥
h4, h1
h0
h0; h1; h3: P
3: ⊥


h0; h1; h3; h5: ¬P
4: ⊥
h0; h1; h3; h6: Q
5: ⊥
h0; h1; h4: Q
6: ⊥
h0; h1; h3: P
3: ⊥
h0; h1: ¬Q
2: ⊥
h0; h2: R
7: ⊥
h0: ¬(P ∧ ¬R)
1: ⊥


[h0; h1; h3; h5] → ⊥
[h0; h1; h3; h6] → ⊥
[h0; h1; h4] → ⊥
[h0; h1; h3] → ⊥
[h0; h1] → ⊥
[h0; h2] → ⊥
[h0] → ⊥


[h0; h1; h3; h5] → ⊥
[h0; h1; h3; h6] → ⊥
[h0; h1; h4] → ⊥
[h0; h1; h3] → ⊥
[h0; h1] → ⊥
[h0; h2] → ⊥
[h0] → ⊥


[h1; h3; h5] → ⊥
[h1; h3; h6] → ⊥
[h1; h4] → ⊥
[h1; h3] → ⊥
[h1] → ⊥
[h2] → ⊥
⊥

Validation

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

- 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 developpers to optimize for goals produced by humans

Questions?

Figure: XKCD 1403

5 Annex

- Trust

Isabelle

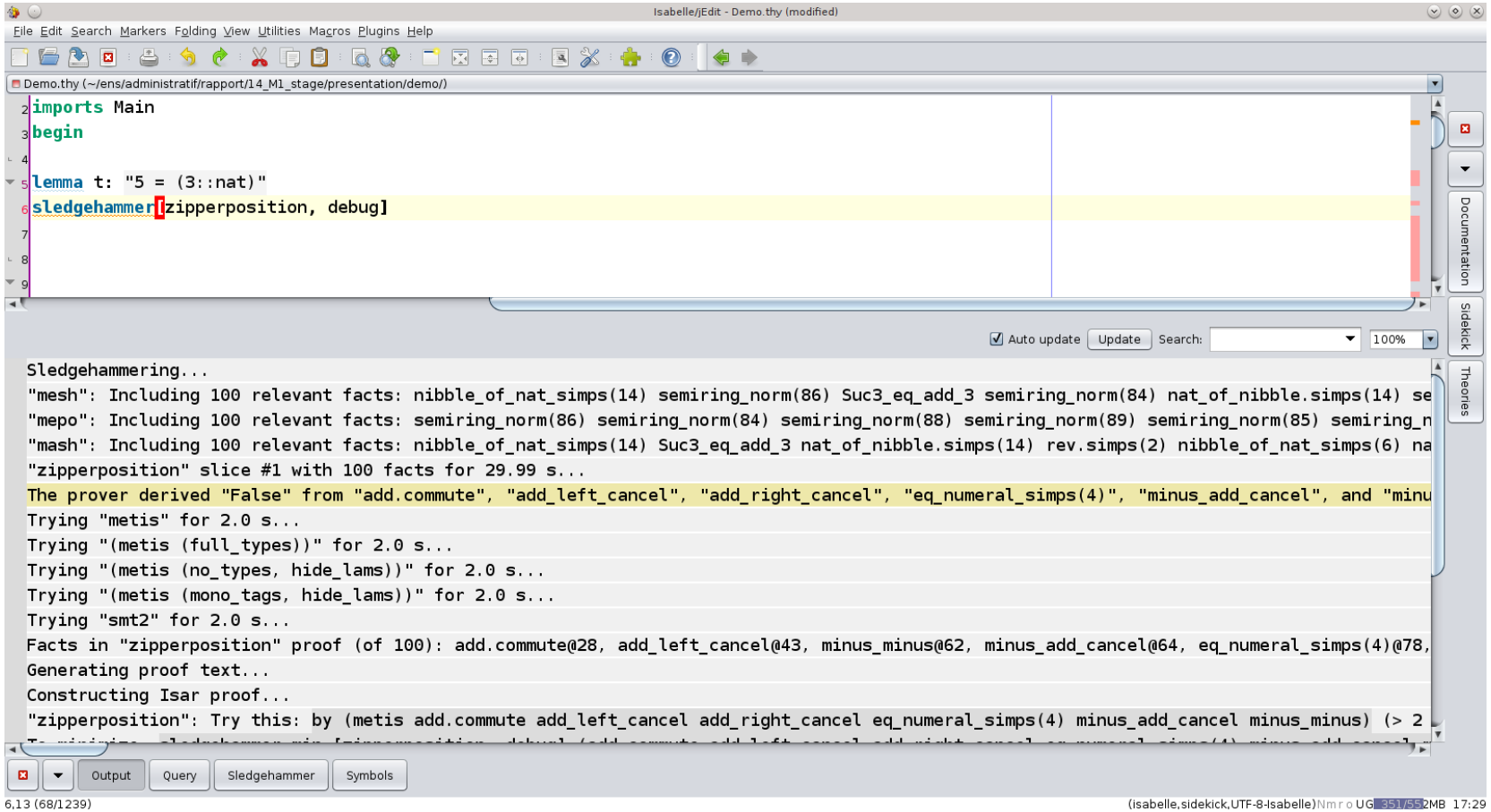


Figure: Isabelle call to Zipperposition through Sledgehammer

Annex

Isabelle

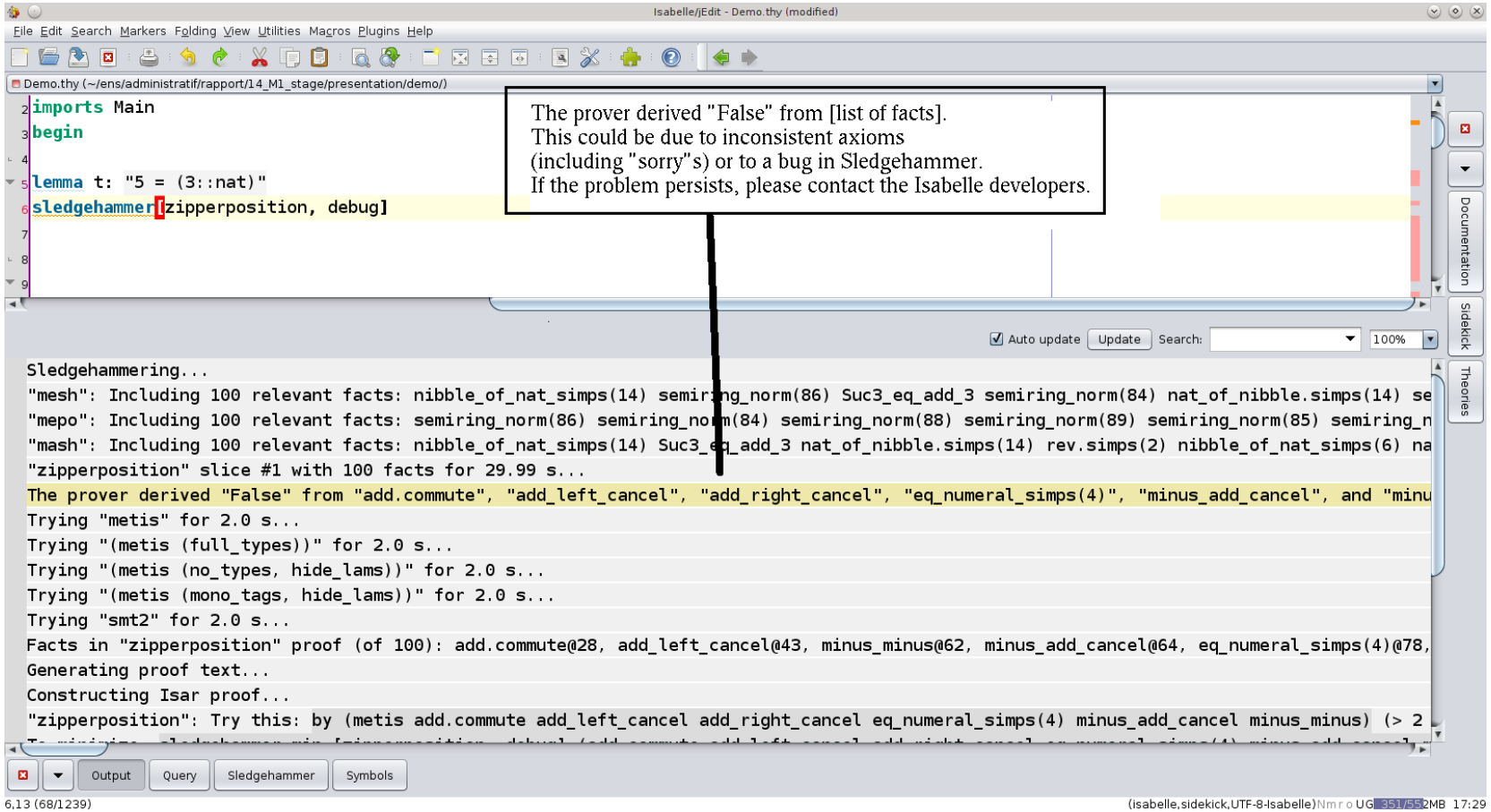


Figure: Isabelle call to Zipperposition through Sledgehammer

Annex

Bugs?

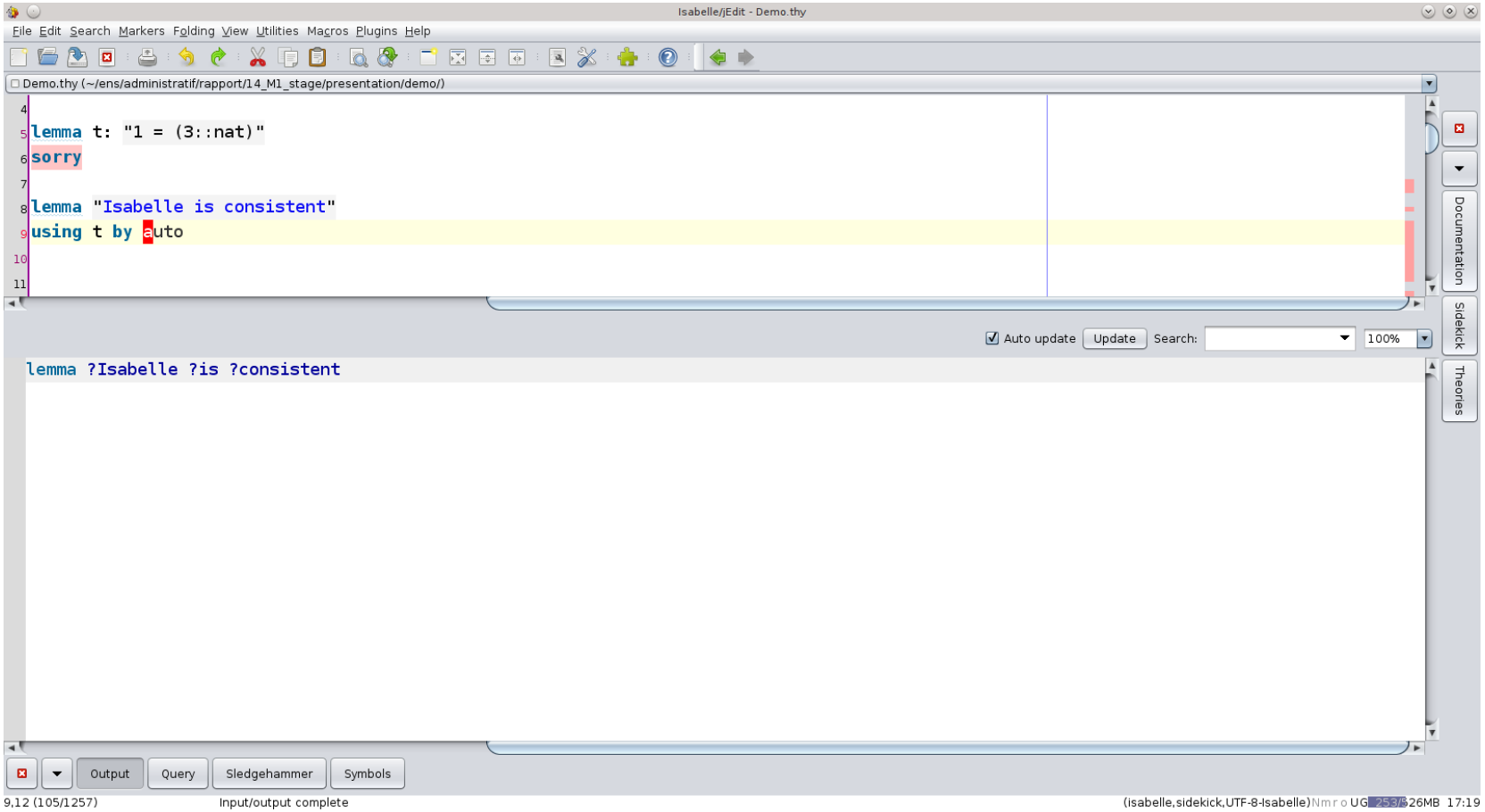


Figure: Isabelle is inconsistent

Annex

Bugs?

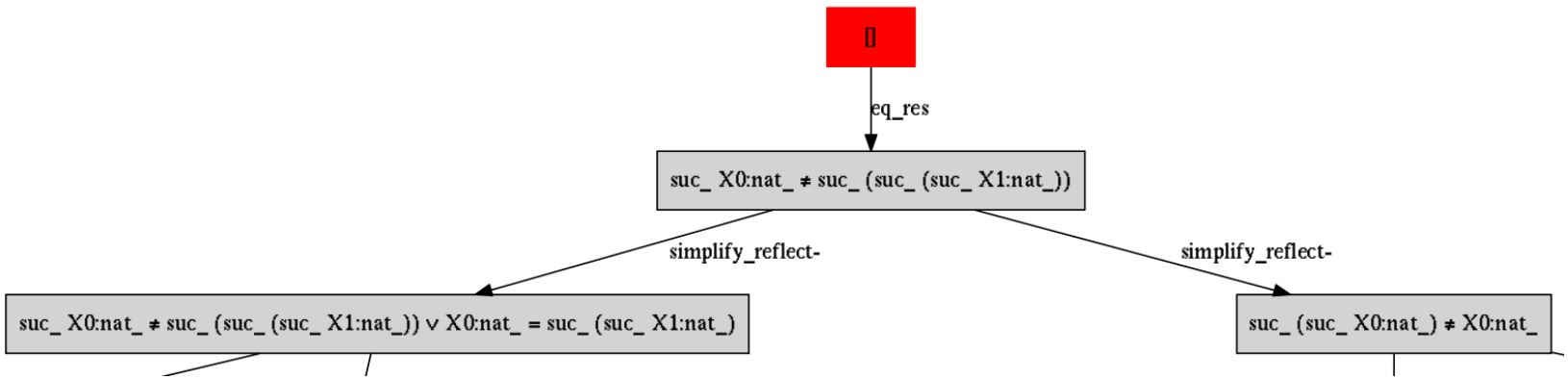


Figure: Zipperposition bug: $\forall X0,\ X1,\ X0 + 1 \neq X1 + 3$, from a consistent set of axioms (Isabelle's nat). It has been corrected.

Annex