Automated Reasoning I

Uwe Waldmann

Winter Term 2019/2020

What is Automated Reasoning?

Automated reasoning:

Logical reasoning using a computer program,

with little or no user interaction,

using general methods, rather than approaches that work only for one specific problem.

Two examples:

Solving a sudoku.

Reasoning with equations.

Introductory Example 1: Sudoku

	1	2	3	4	5	6	7	8	9
1								1	
2	4								
3		2							
4					5		4		7
5			8				3		
6			1		9				
7	3			4			2		
8		5		1					
9				8		6			

Goal:

Fill the empty fields with digits 1,. . . ,9 so that each digit occurs exactly once in each row, column, and 3×3 box

Introductory Example 1: Sudoku

	1	2	3	4	5	6	7	8	9
1								1	
2	4								
3		2							
4					5		4		7
5			8				3		
6			1		9				
7	3			4			2		
8		5		1					
9				8		6			

Idea:

Use boolean variables $P^d_{i,j}$ with $d, i, j \in \{1, \dots, 9\}$ to encode the problem:

$P^d_{i,j}$=true iff the value of square i, j is d

Introductory Example 1: Sudoku

	1	2	3	4	5	6	7	8	9
1								1	
2	4								
3		2							
4					5		4		7
5			8				3		
6			1		9				
7	3			4			2		
8		5		1					
9				8		6			

Idea:

Use boolean variables $P^d_{i,j}$ with $d, i, j \in \{1, \ldots, 9\}$ to encode the problem:

$P^d_{i,j}$=true iff the value of square i, j is d

For example:

$$P^8_{5,3} = true$$

Coding Sudoku in Boolean Logic

- Concrete values result in formulas $P^d_{i,j}$
- For every square (i,j) we generate $P^1_{i,j} \vee \ldots \vee P^9_{i,j}$
- For every square (i,j) and pair of values $d < d'$ we generate $\neg P^d_{i,j} \vee \neg P^{d'}_{i,j}$
- For every value d and row i we generate $P^d_{i,1} \vee \ldots \vee P^d_{i,9}$
  (Analogously for columns and 3×3 boxes)
- For every value d, row i, and pair of columns $j < j'$
  we generate $\neg P^d_{i,j} \vee \neg P^d_{i,j'}$
  (Analogously for columns and 3×3 boxes)

Coding Sudoku in Boolean Logic

Every assignment of boolean values to the variables $P^d_{i,j}$
so that all formulas become true
corresponds to a Sudoku solution (and vice versa).

Coding Sudoku in Boolean Logic

Now use a SAT solver to check whether there is an assignment to the variables $P_{i,j}^{d}$ so that all formulas become true:

Niklas Eén, Niklas Sörensson:
MiniSat (`http://minisat.se/`),

Beware:

The satisfiability problem is NP-complete.

Every known algorithm to solve it has an exponential time worst-case behaviour (or worse).

Coding Sudoku in Boolean Logic

MiniSat solves the problem in a few milliseconds.

How? See part 2 of this lecture.

Does that contradict NP-completeness? No!

NP-completeness implies that there are really hard problem instances,

it does not imply that all practically interesting problem instances are hard (for a well-written SAT solver).

SAT Solvers in Practice

Some real-life applications of modern SAT solvers:

hardware verification (model checking)

with extensions:

software verification, hybrid system verification, ...

checking software package dependencies

solving combinatory problems

"The Largest Math Proof Ever" (Marijn Heule)

...

Introductory Example 2: Equations

Task:

Prove: $$\frac{a}{a+1} \;=\; 1 + \frac{-1}{a+1}.$$

Introductory Example 2: Equations

$$\frac{a}{a+1}$$

$$1 + \frac{-1}{a+1}$$

Introductory Example 2: Equations

$$\frac{a}{a+1} = \frac{a+0}{a+1}$$

$$x + 0 = x \qquad (1)$$

$$1 + \frac{-1}{a+1}$$

Introductory Example 2: Equations

$$\frac{a}{a+1} = \frac{a+0}{a+1}$$

$$= \frac{a+(1+(-1))}{a+1}$$

$$1 + \frac{-1}{a+1}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

Introductory Example 2: Equations

$$\frac{a}{a+1} = \frac{a+0}{a+1}$$

$$= \frac{a+(1+(-1))}{a+1}$$

$$= \frac{(a+1)+(-1)}{a+1}$$

$$1 + \frac{-1}{a+1}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

Introductory Example 2: Equations

$$
\begin{aligned}
\frac{a}{a+1} &= \frac{a+0}{a+1} \\
&= \frac{a+(1+(-1))}{a+1} \\
&= \frac{(a+1)+(-1)}{a+1} \\
&= \frac{a+1}{a+1} + \frac{-1}{a+1} \\
& 1 + \frac{-1}{a+1}
\end{aligned}
$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{4}$$

Introductory Example 2: Equations

$$\begin{aligned}
\frac{a}{a+1} &= \frac{a+0}{a+1} \\
&= \frac{a+(1+(-1))}{a+1} \\
&= \frac{(a+1)+(-1)}{a+1} \\
&= \frac{a+1}{a+1} + \frac{-1}{a+1} \\
&= 1 + \frac{-1}{a+1}
\end{aligned}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

How could we write a program that takes a set of equations and two terms and tests whether the terms can be connected via a chain of equalities?

It is easy to write a program that applies formulas *correctly*.

But: correct $\neq$ useful.

Introductory Example 2: Equations

$$\frac{a}{a+1}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x + y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

$$\frac{a}{a+1} \longrightarrow \frac{a+0}{a+1}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

$$\begin{tikzcd} \dfrac{a}{a+1} \arrow[r] \arrow[dr] & \dfrac{a+0}{a+1} \\ & \dfrac{a}{a+1}+0 \end{tikzcd}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

$$\frac{a}{a+1} \longrightarrow \frac{a+0}{a+1}$$

$$\frac{a}{a+1} \longrightarrow \frac{a}{a+1} + 0$$

$$\frac{a}{a+1} \longrightarrow \frac{a}{a+(1+0)}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

$$\begin{tikzcd} \frac{a}{a+1} \arrow[r] \arrow[dr] \arrow[ddr] \arrow[dddr] & \frac{a+0}{a+1} \\ & \frac{a}{a+1}+0 \\ & \frac{a}{a+(1+0)} \\ & \frac{a}{a+\frac{a+2}{a+2}} \end{tikzcd}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x + y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

$$\frac{a}{a+1} \longrightarrow \frac{a+0}{a+1}$$

$$\frac{a}{a+1} + 0$$

$$\frac{a}{a+(1+0)}$$

$$\frac{a}{a+\frac{a+2}{a+2}}$$

$$\vdots$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

$$1 + \frac{-1}{a+1}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

$$1 + \frac{-1}{a+1} \longrightarrow \frac{a+1}{a+1} + \frac{-1}{a+1}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

$$1 + \frac{-1}{a+1} \longrightarrow \frac{a+1}{a+1} + \frac{-1}{a+1}$$

$$\frac{a}{a} + \frac{-1}{a+1}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

$$1 + \frac{-1}{a+1} \longrightarrow \frac{a+1}{a+1} + \frac{-1}{a+1}$$

$$\frac{a}{a} + \frac{-1}{a+1}$$

$$1 + \frac{-1}{a + \frac{a}{a}}$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x + y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

$$\begin{tikzcd} 1+\frac{-1}{a+1} \arrow[r] \arrow[dr] \arrow[ddr] \arrow[dddr] & \frac{a+1}{a+1}+\frac{-1}{a+1} \\ & \frac{a}{a}+\frac{-1}{a+1} \\ & 1+\frac{-1}{a+\frac{a}{a}} \\ & 1+\frac{-1+0}{a+1} \end{tikzcd}$$

$$x+0=x \tag{1}$$

$$x+(-x)=0 \tag{2}$$

$$x+(y+z)=(x+y)+z \tag{3}$$

$$\frac{x}{z}+\frac{y}{z}=\frac{x+y}{z} \tag{4}$$

$$\frac{x}{x}=1 \tag{5}$$

Introductory Example 2: Equations

$$
\begin{array}{rl}
1 + \dfrac{-1}{a+1} & \longrightarrow \dfrac{a+1}{a+1} + \dfrac{-1}{a+1} \\[2ex]
& \longrightarrow \dfrac{a}{a} + \dfrac{-1}{a+1} \\[2ex]
& \longrightarrow 1 + \dfrac{-1}{a + \frac{a}{a}} \\[2ex]
& \longrightarrow 1 + \dfrac{-1+0}{a+1} \\[2ex]
& \longrightarrow \vdots
\end{array}
$$

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

Unrestricted application of equations leads to

- infinitely many equality chains,
- infinitely long equality chains.

$\Rightarrow$ The chance to reach the desired goal is very small.

In fact, the general problem is only recursively enumerable, but not decidable.

Introductory Example 2: Equations

A better approach:

Apply equations in such a way that terms become "simpler".

Start from both sides:

-
-

Introductory Example 2: Equations

A better approach:

Apply equations in such a way that terms become "simpler".

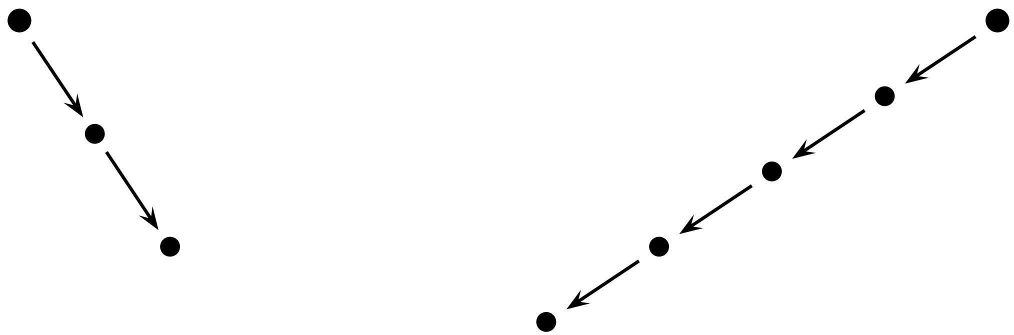
Start from both sides:

Introductory Example 2: Equations

A better approach:

Apply equations in such a way that terms become “simpler”.

Start from both sides:

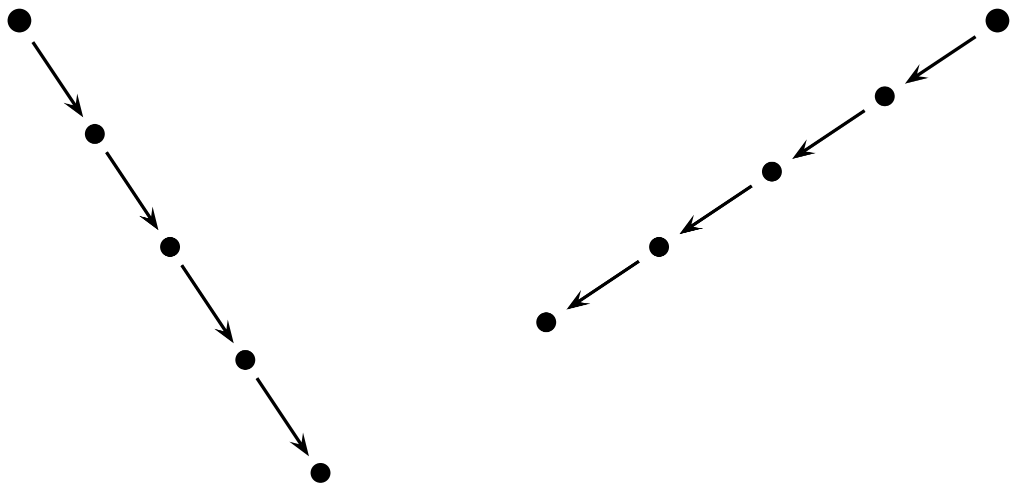


Introductory Example 2: Equations

A better approach:

Apply equations in such a way that terms become “simpler”.

Start from both sides:

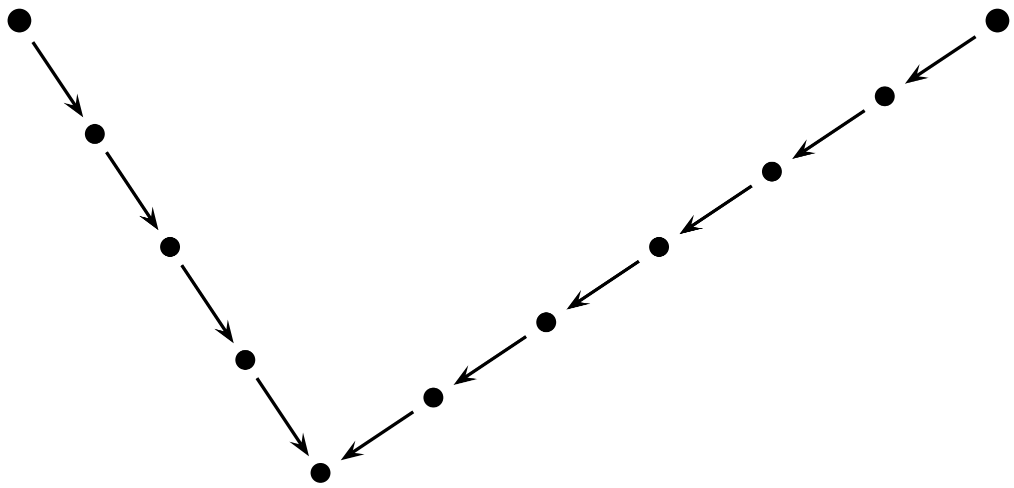


Introductory Example 2: Equations

A better approach:

Apply equations in such a way that terms become "simpler".

Start from both sides:



The terms are equal, if both derivations meet.

Introductory Example 2: Equations

$$x + 0 = x \tag{1}$$

$$x + (-x) = 0 \tag{2}$$

$$x + (y + z) = (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} = \frac{x + y}{z} \tag{4}$$

$$\frac{x}{x} = 1 \tag{5}$$

Introductory Example 2: Equations

Orient equations.

$$x + 0 \to x \tag{1}$$

$$x + (-x) \to 0 \tag{2}$$

$$x + (y + z) \to (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} \to \frac{x + y}{z} \tag{4}$$

$$\frac{x}{x} \to 1 \tag{5}$$

Introductory Example 2: Equations

Orient equations.

Advantage:
Now there are only finitely many and finitely long derivations.

$$x + 0 \to x \tag{1}$$

$$x + (-x) \to 0 \tag{2}$$

$$x + (y + z) \to (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} \to \frac{x + y}{z} \tag{4}$$

$$\frac{x}{x} \to 1 \tag{5}$$

Introductory Example 2: Equations

Orient equations.

But:
Now none of the equations is applicable to one of the terms

$$\frac{a}{a+1}, \quad 1 + \frac{-1}{a+1}$$

$$x + 0 \to x \tag{1}$$

$$x + (-x) \to 0 \tag{2}$$

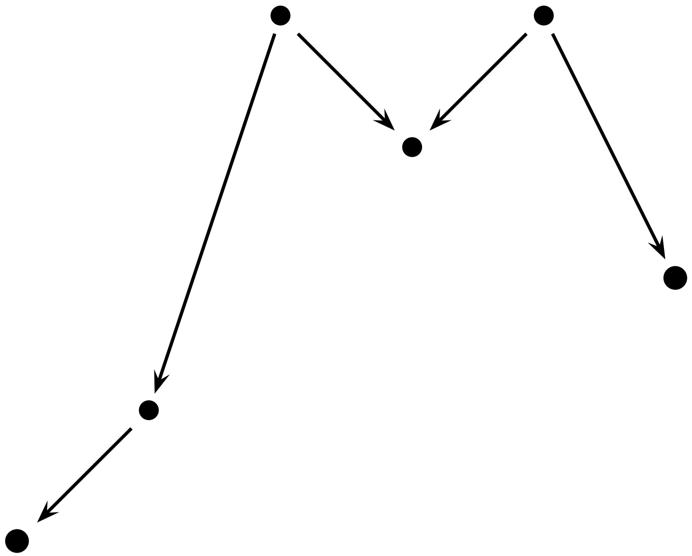
$$x + (y + z) \to (x + y) + z \tag{3}$$

$$\frac{x}{z} + \frac{y}{z} \to \frac{x + y}{z} \tag{4}$$

$$\frac{x}{x} \to 1 \tag{5}$$

Introductory Example 2: Equations

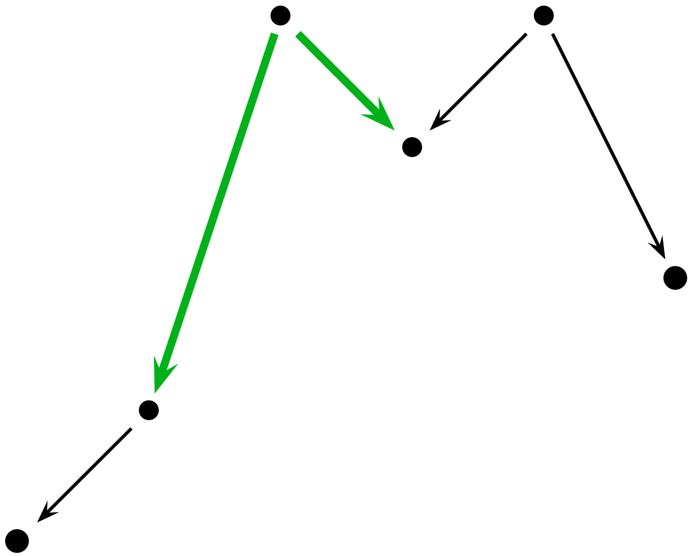
The chain of equalities that we considered at the beginning looks roughly like this:



Introductory Example 2: Equations

Idea:

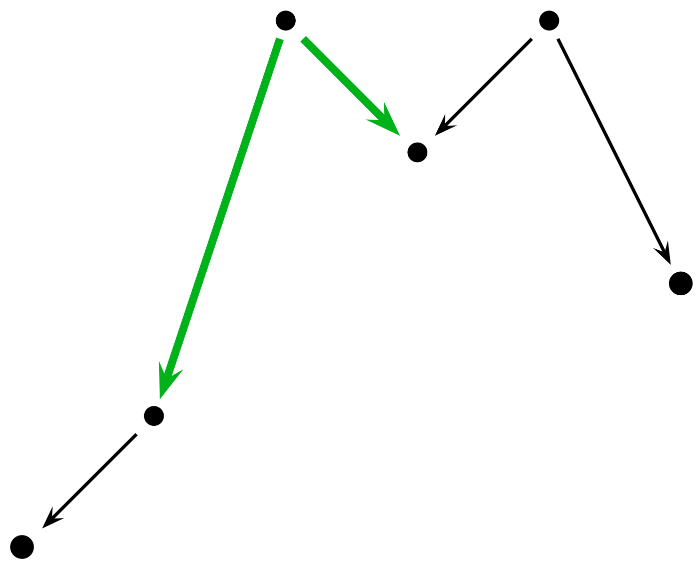
Derive new equations that enable “shortcuts”.



Introductory Example 2: Equations

Idea:

Derive new equations that enable “shortcuts”.



From

$$x + (-x) \to 0 \qquad (2)$$

$$x + (y + z) \to (x + y) + z \qquad (3)$$

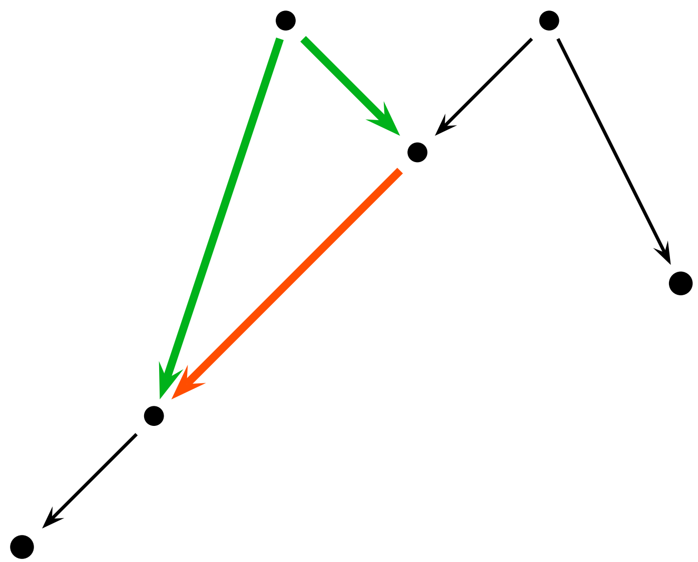
we derive

$$(x + y) + (-y) \to x + 0 \qquad (6)$$

Introductory Example 2: Equations

Idea:

Derive new equations that enable “shortcuts”.



From

$$x + (-x) \to 0 \qquad (2)$$

$$x + (y + z) \to (x + y) + z \qquad (3)$$

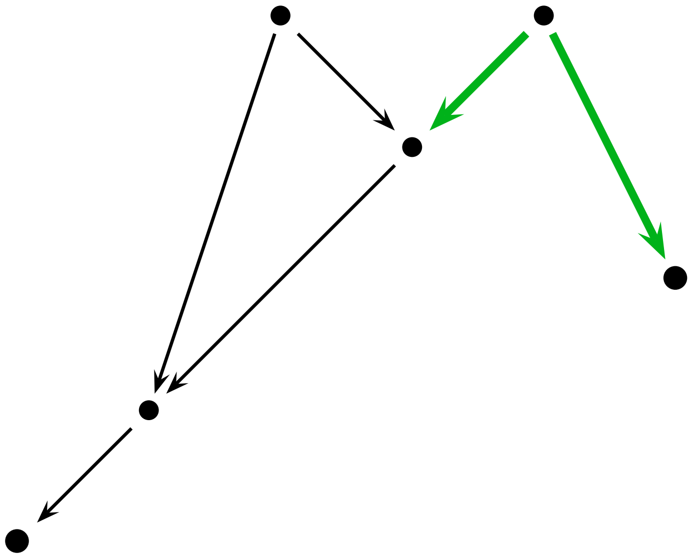
we derive

$$(x + y) + (-y) \to x + 0 \qquad (6)$$

Introductory Example 2: Equations

Idea:

Derive new equations that enable "shortcuts".



From

$$\frac{x}{z} + \frac{y}{z} \to \frac{x+y}{z} \tag{4}$$

$$\frac{x}{x} \to 1 \tag{5}$$

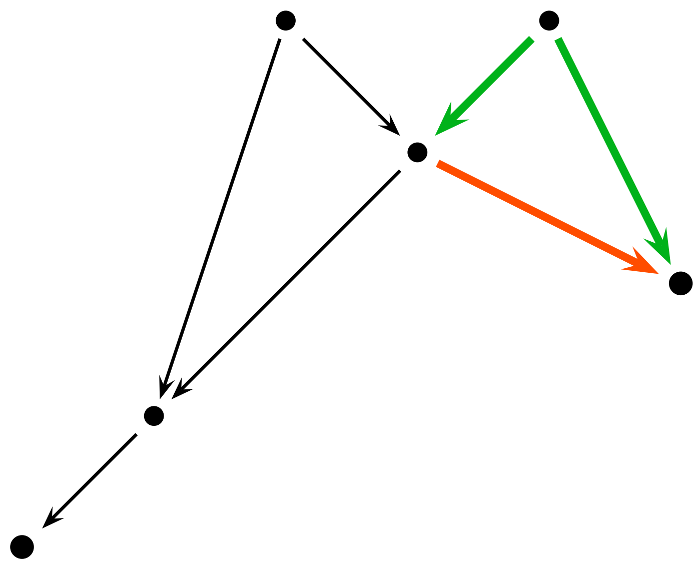
we derive

$$\frac{x+y}{x} \to 1 + \frac{y}{x} \tag{7}$$

Introductory Example 2: Equations

Idea:

Derive new equations that enable “shortcuts”.



From

$$\frac{x}{z} + \frac{y}{z} \to \frac{x+y}{z} \qquad (4)$$

$$\frac{x}{x} \to 1 \qquad (5)$$

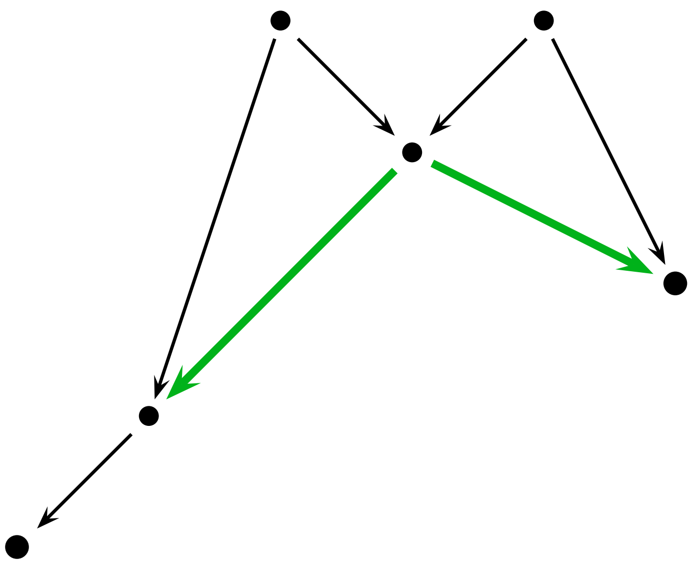
we derive

$$\frac{x+y}{x} \to 1 + \frac{y}{x} \qquad (7)$$

Introductory Example 2: Equations

Idea:

Derive new equations that enable "shortcuts".



From

$$(x+y)+(-y) \to x+0 \tag{6}$$

$$\frac{x+y}{x} \to 1+\frac{y}{x} \tag{7}$$

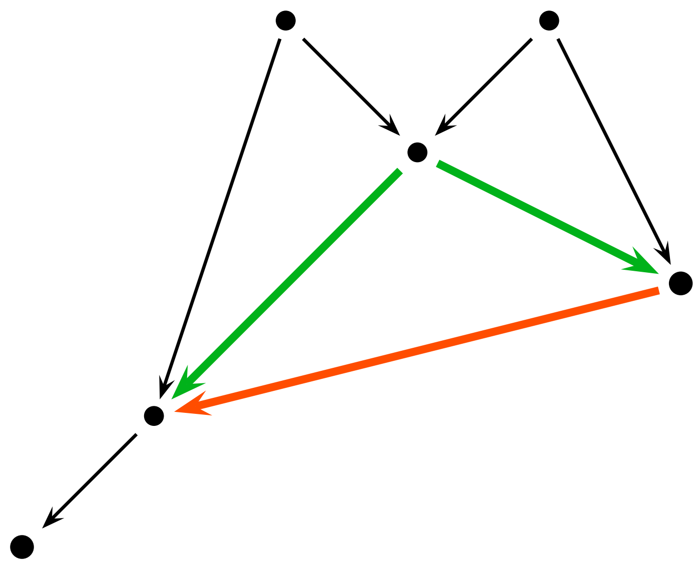
we derive

$$1+\frac{-y}{x+y} \to \frac{x+0}{x+y} \tag{8}$$

Introductory Example 2: Equations

Idea:

Derive new equations that enable "shortcuts".



From

$$(x + y) + (-y) \to x + 0 \qquad (6)$$

$$\frac{x + y}{x} \to 1 + \frac{y}{x} \qquad (7)$$

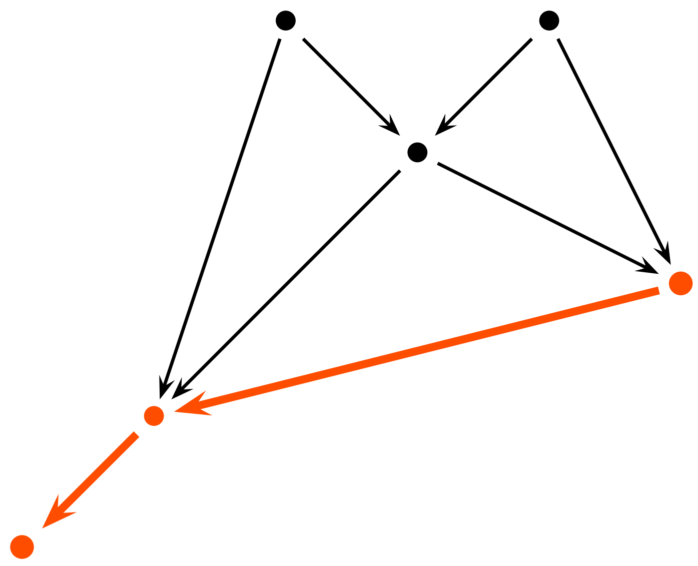
we derive

$$1 + \frac{-y}{x + y} \to \frac{x + 0}{x + y} \qquad (8)$$

Introductory Example 2: Equations

Idea:

Derive new equations that enable “shortcuts”.



Using these equations we can get a chain of equalities of the desired form.

Introductory Example 2: Equations

In fact, it is not necessary to know some equational proof for the problem in advance.

We can derive these shortcut equations just by looking at the existing equation set.

How? See part 4 of this lecture.

Result

Waldmeister

(Thomas Hilenbrand,
`https://www.mpi-inf.mpg.de/departments/automation-of-logic/software/waldmeister/`)

solves the problem in a few milliseconds.

Result

But it's not the solution that we wanted to get!

We have to be more careful in formulating our axioms:

$\Rightarrow$ Exclude division by zero.

Then we get in fact a "real" proof.

Result

So it works, but it looks like a lot of effort for a problem that one can solve with a little bit of highschool mathematics.

Reason: Pupils learn not only axioms, but also recipes
to work efficiently with these axioms.

Result

It makes a huge difference whether we work with well-known axioms

$$x + 0 = x$$
$$x + (-x) = 0$$

or with “new” unknown ones

$$\begin{aligned} &\forall Agent\ \forall Message\ \forall Key. \\ &\qquad knows(Agent, crypt(Message, Key)) \\ &\qquad \wedge\ knows(Agent, Key) \\ &\qquad \rightarrow\ knows(Agent, Message). \end{aligned}$$

Result

This difference is also important for automated reasoning:

- For axioms that are well-known and frequently used, we can develop optimal specialized methods.
  $\Rightarrow$ Computer Algebra
  $\Rightarrow$ Automated Reasoning II (next semester)

- For new axioms, we have to develop methods that do "something reasonable" for arbitrary formulas.
  $\Rightarrow$ this lecture

- Combining the two approaches
  $\Rightarrow$ Automated Reasoning II

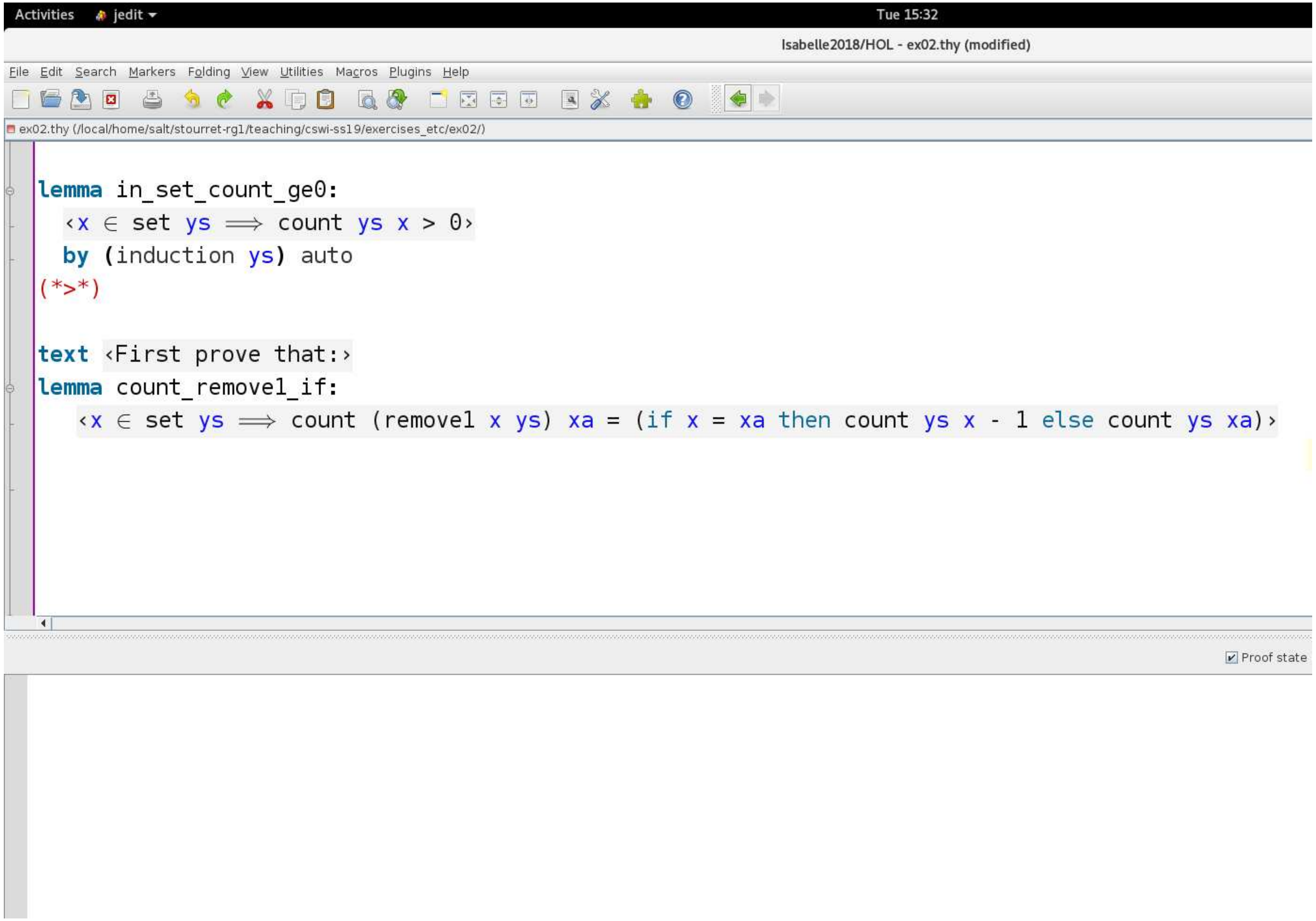
First-order Provers in Practice

Real-life application:

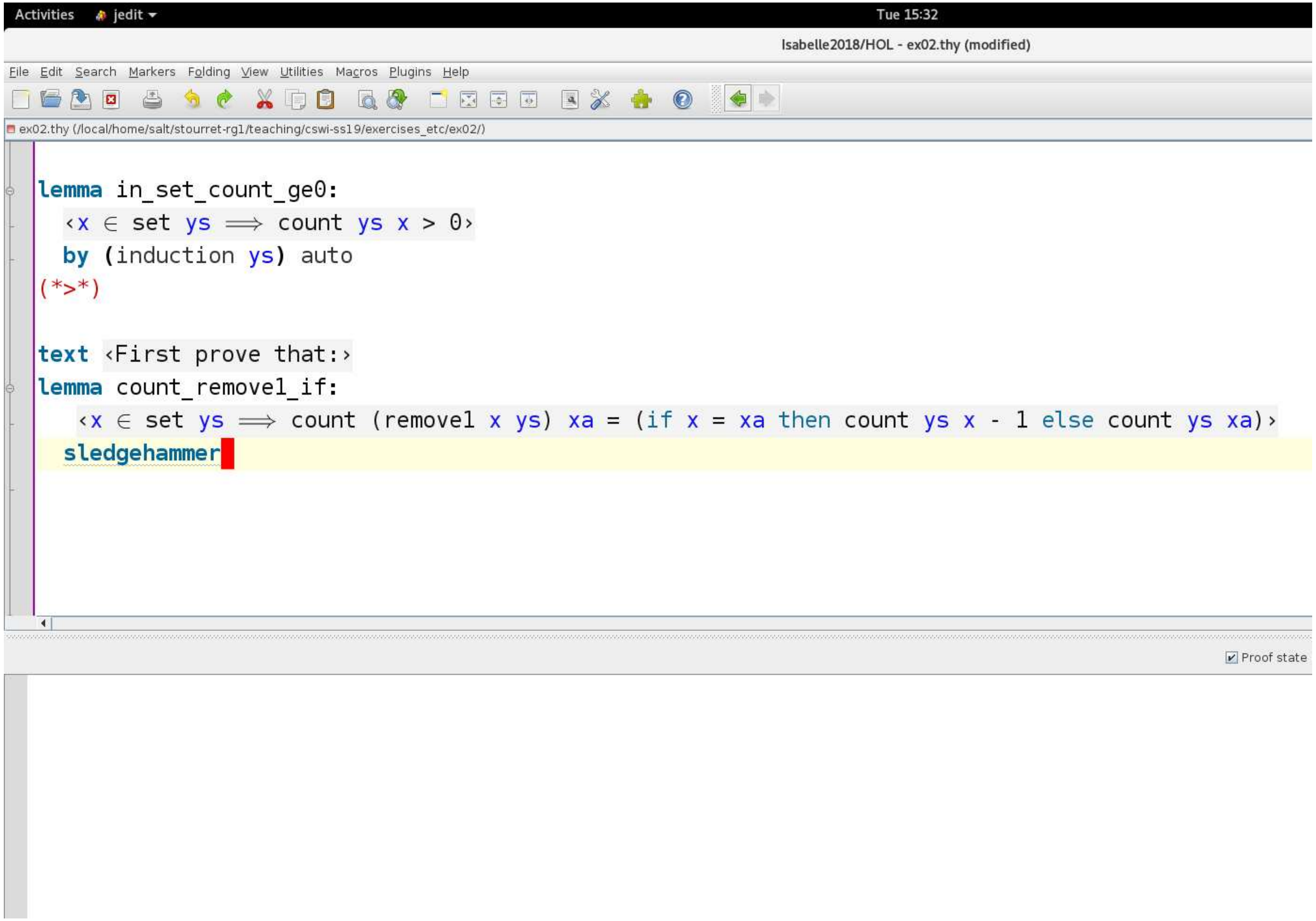
Isabelle tactic "Sledgehammer":

use general-purpose provers to make interactive proof assistants more automatic.

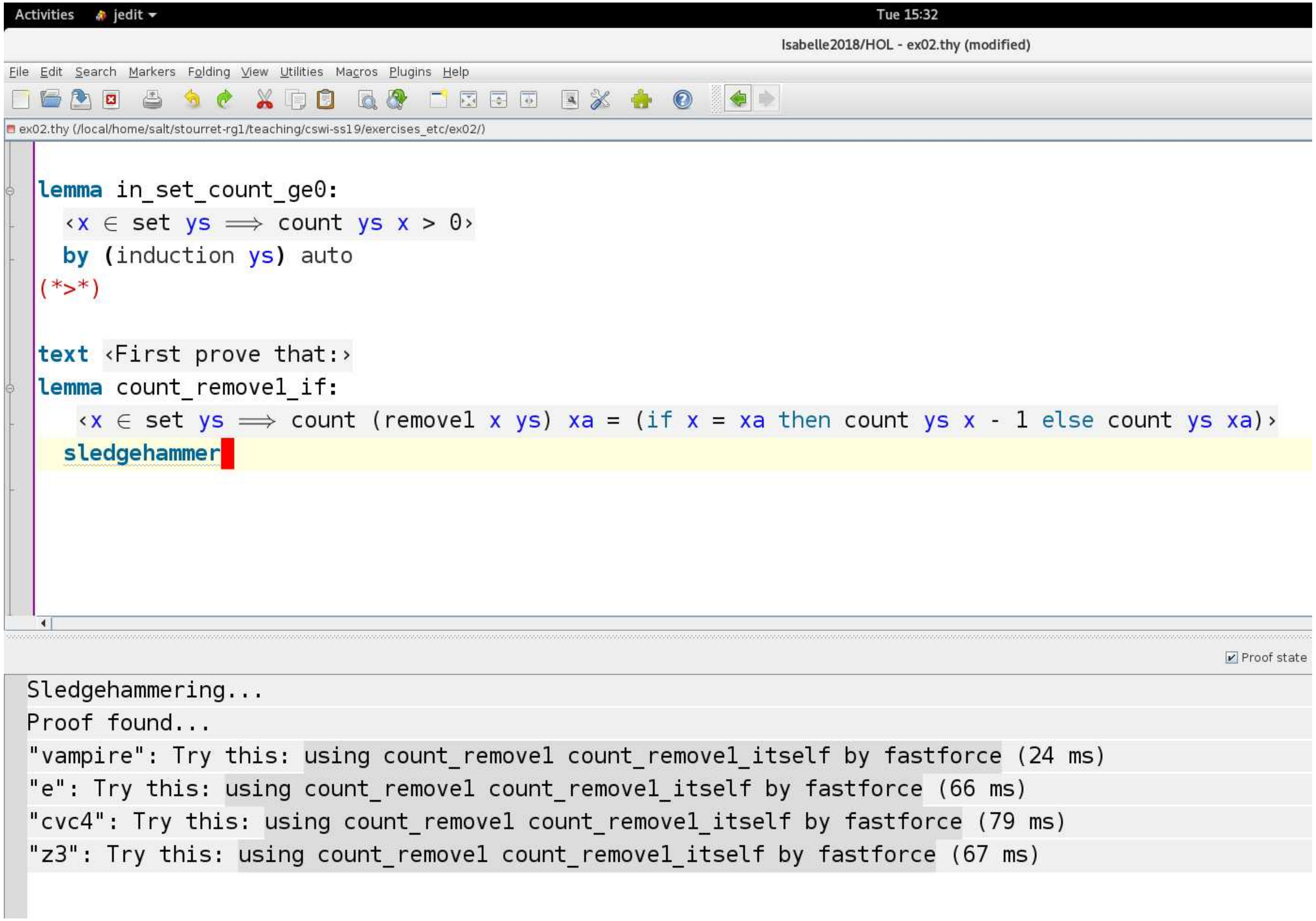
First-order Provers in Practice



First-order Provers in Practice



First-order Provers in Practice



First-order Provers in Practice