What is Automated Deduction?

Automated deduction:

Logical reasoning using a computer program.

Introductory Example

Task:

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

Introductory Example

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

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

Introductory Example

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

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

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

Introductory Example

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

Introductory Example

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

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

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

$$\frac{a}{a+1} \longrightarrow \frac{a}{a+\frac{a+2}{a+2}}$$

$$\vdots$$

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

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

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

Introductory Example

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

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

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

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

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

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

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

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

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

Introductory Example

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

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

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

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

$$\vdots$$

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

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

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

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

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

Introductory Example

Unrestricted application of equations leads to

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

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

Introductory Example

A better approach:

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

Start from both sides:

-
-

Introductory Example

A better approach:

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

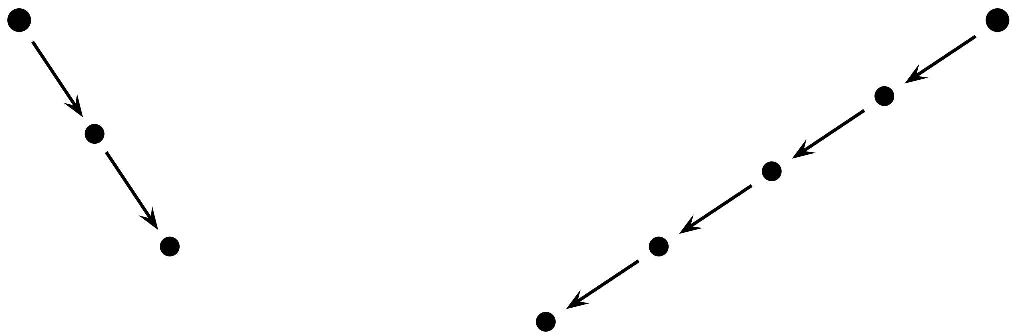
Start from both sides:

Introductory Example

A better approach:

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

Start from both sides:

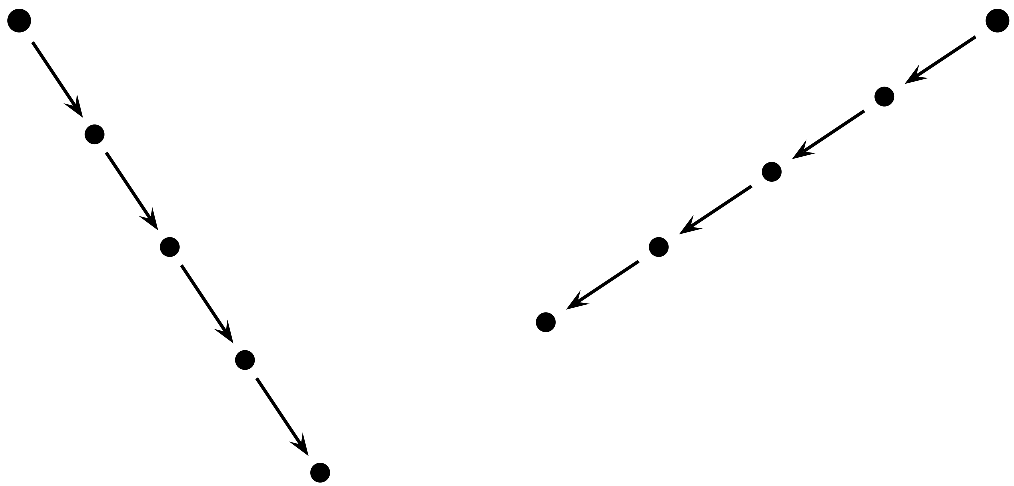


Introductory Example

A better approach:

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

Start from both sides:

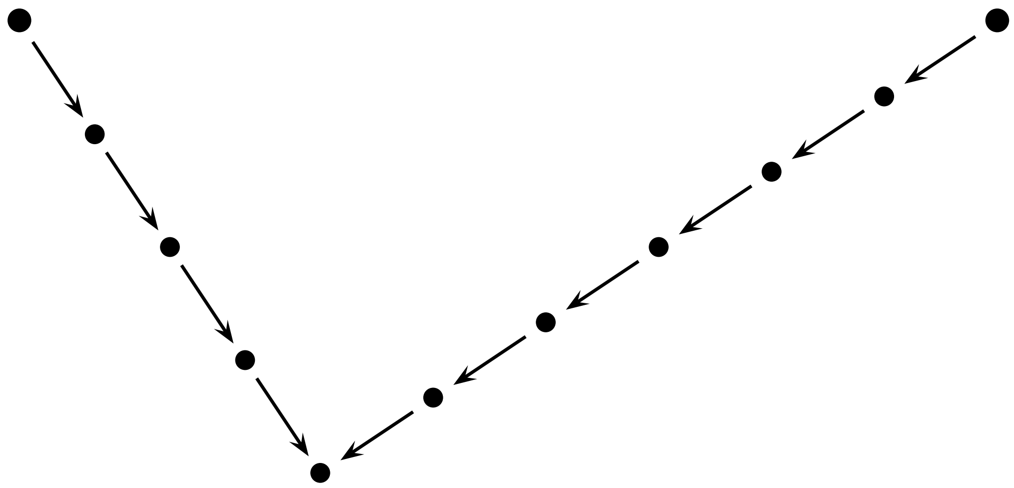


Introductory Example

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

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

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

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

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

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

Introductory Example

Orient equations.

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

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

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

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

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

Introductory Example

Orient equations.

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

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

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

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

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

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

Introductory Example

Orient equations.

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

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

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

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

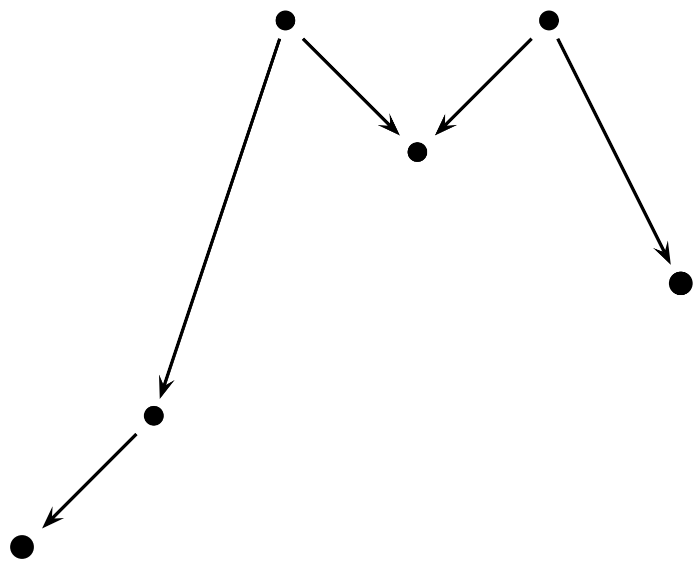
$$x + (y + z) \to (x + y) + z \tag{3}$$

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

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

Introductory Example

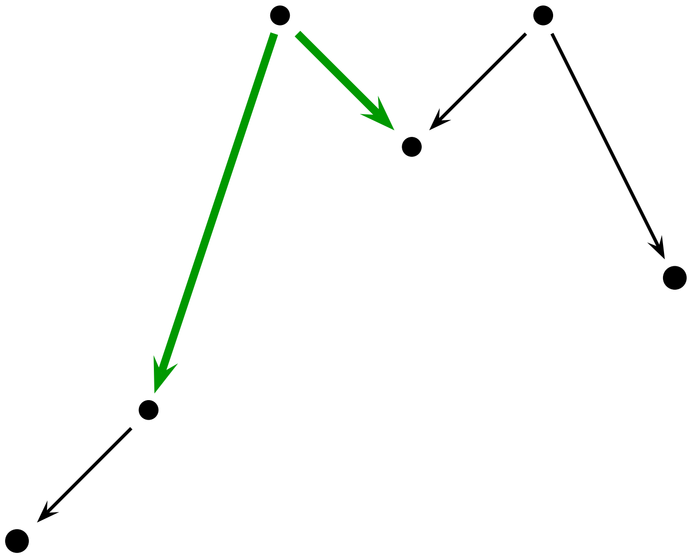
The chain of equalities we considered at the beginning looks roughly like this:



Introductory Example

Idea:

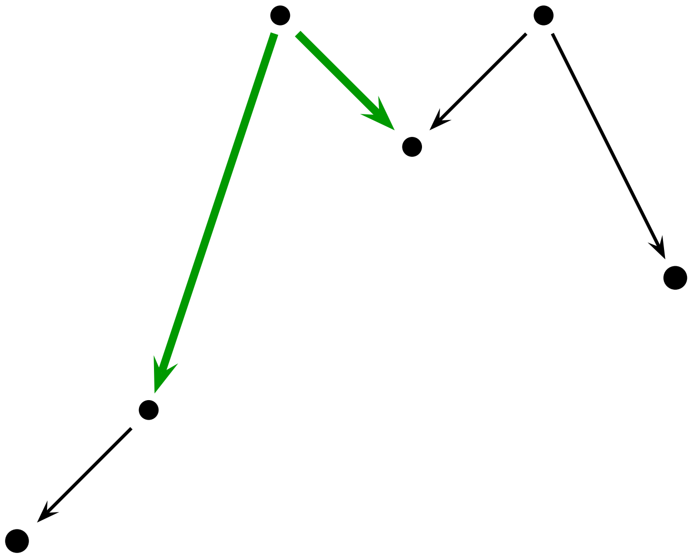
Derive new equations that enable “shortcuts”.



Introductory Example

Idea:

Derive new equations that enable "shortcuts".



From

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

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

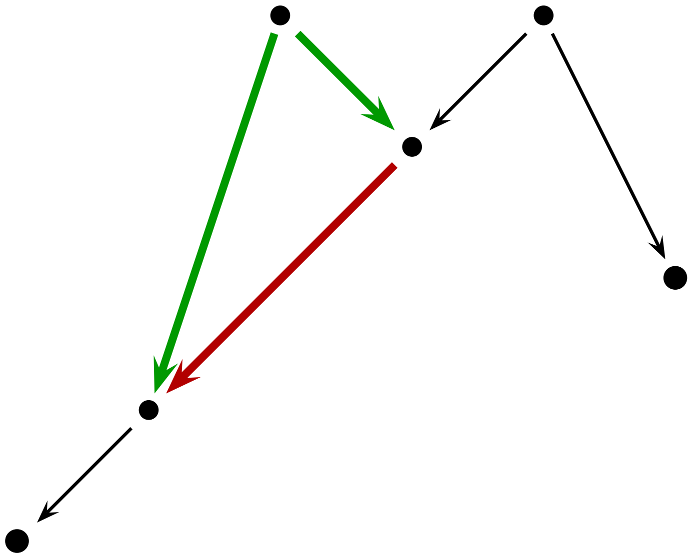
we derive

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

Introductory Example

Idea:

Derive new equations that enable "shortcuts".



From

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

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

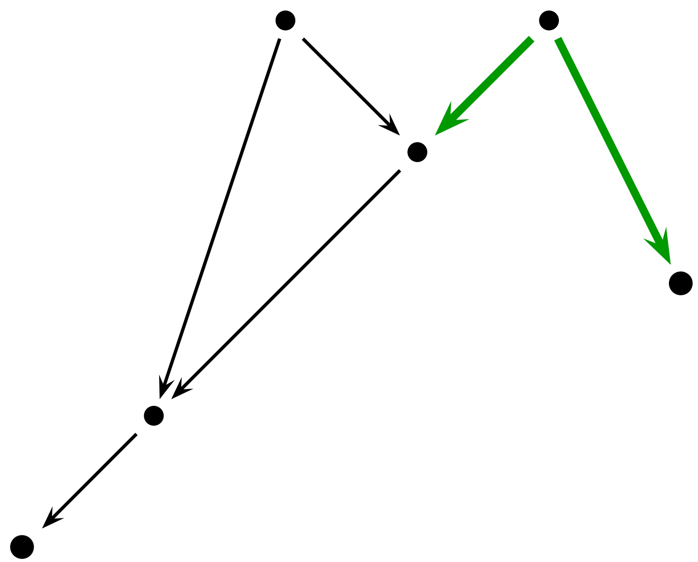
we derive

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

Introductory Example

Idea:

Derive new equations that enable “shortcuts”.



From

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

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

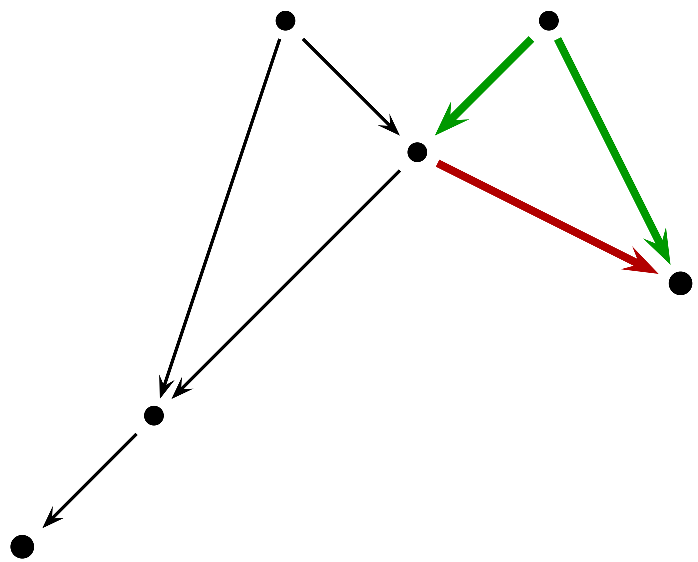
we derive

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

Introductory Example

Idea:

Derive new equations that enable “shortcuts”.



From

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

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

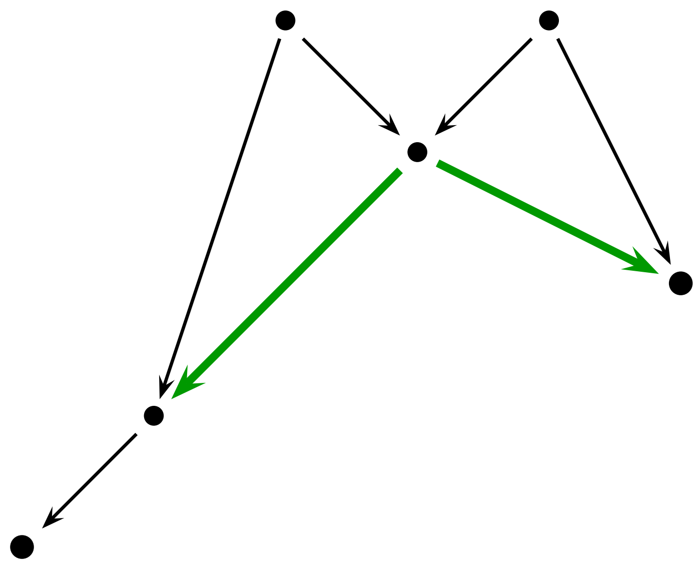
we derive

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

Introductory Example

Idea:

Derive new equations that enable "shortcuts".



From

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

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

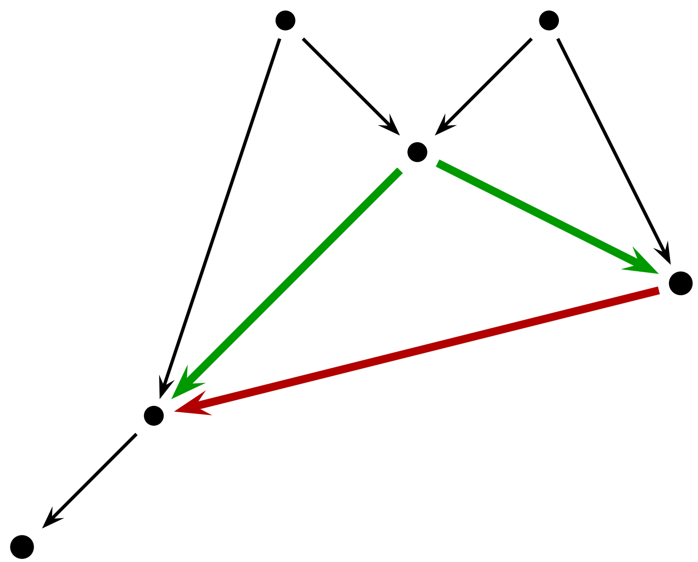
we derive

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

Introductory Example

Idea:

Derive new equations that enable "shortcuts".



From

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

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

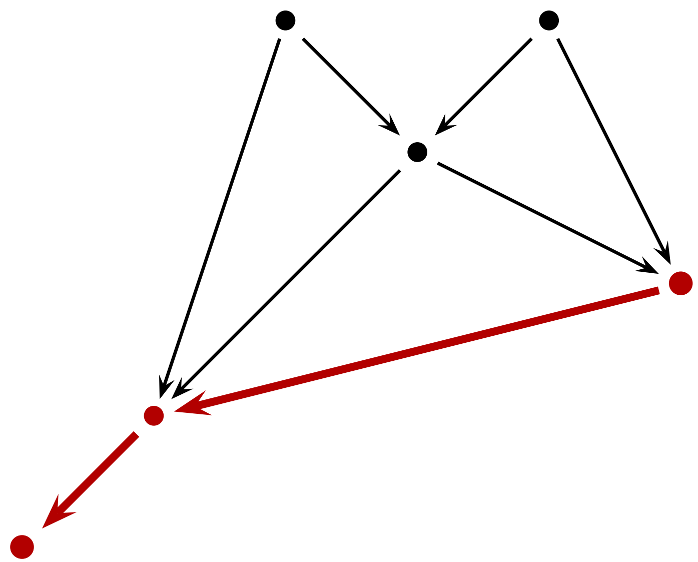
we derive

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

Introductory Example

Idea:

Derive new equations that enable “shortcuts”.



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

Result

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.
  $\Rightarrow$ Selected Topics in Aut. Reas. (V. Sofronie-Stokkermans)
  $\Rightarrow$ Computer Algebra (M. Sagraloff)

- 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 (next semester)