Introduction to Cyclic Proofs

Liron Cohen

LMW 2022 @CSL

cliron@cs.bgu.ac.il

Q: How do we know something is true?

A: We prove it

Q: How do we know that we have a proof?

A: We need to define what it means to be a proof.

A proof is a logical sequence of arguments, starting from some initial assumptions (axioms)

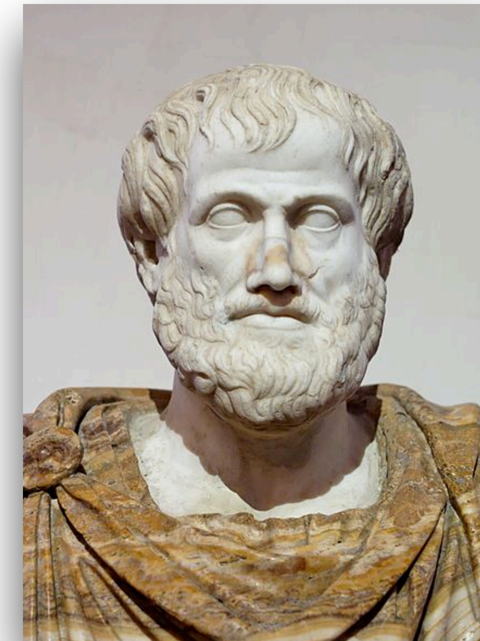
Q: How do we know that we have a valid sequence of arguments? Can any sequence be a proof? E.g.

All humans are mortal

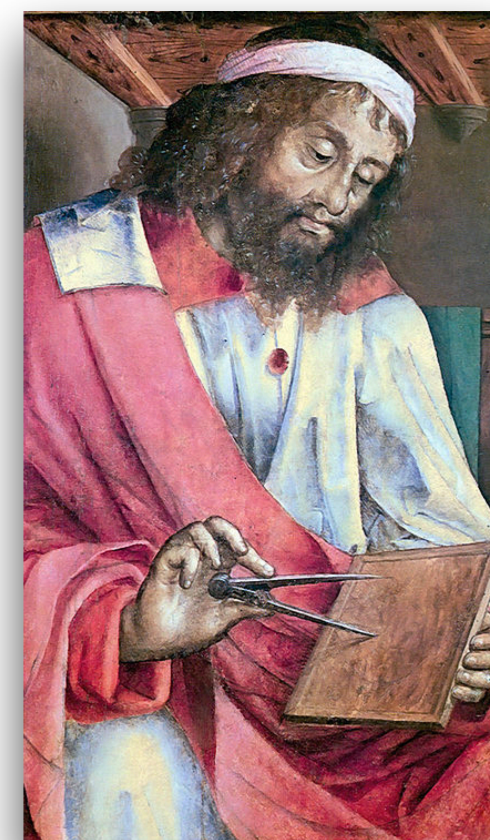
All Greeks are human

Therefore I am a Greek!

A: No! We must think harder about valid ways of reasoning



Aristotle
384 – 322 BC



Euclid
~300 BC

The Good Old Notion of a Proof

How Do We Prove?

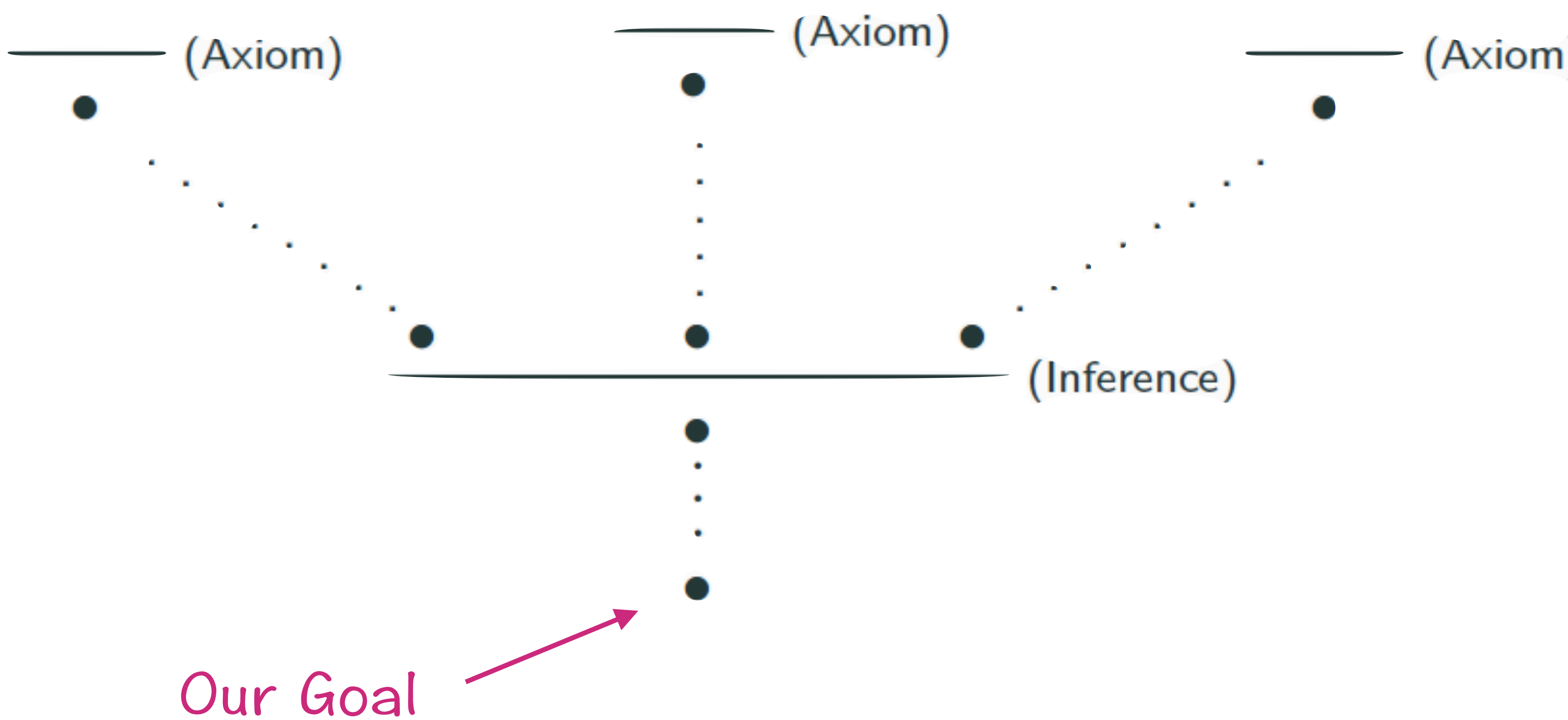
"A proof is a proof.
What kind of a proof?
It's a proof.
A proof is a proof,
and when you have a good proof,
it's because it's proven."
— Jean Chretien

Proof by cases
Proof by contradiction
Proof by Induction
...

Classical Proof
Constructive Proof
Intuitionistic proof
...

Proofs using sequent calculus
Proofs in natural deduction
...

What is a Formal Proof?



Soundness: If the axioms are sound and every inference rule is sound, then every proof is sound.

The System LK [Gentzen, '34]

$$\frac{\psi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}\ (\wedge L_1) \qquad \frac{\varphi, \Gamma \Rightarrow \Delta}{\varphi \wedge \psi, \Gamma \Rightarrow \Delta}\ (\wedge L_2) \qquad \frac{\Gamma \Rightarrow \Delta, \varphi \quad \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \wedge \psi}\ (\wedge R)$$

$$\frac{\varphi, \Gamma \Rightarrow \Delta \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \vee \psi, \Gamma \Rightarrow \Delta}\ (\vee L) \qquad \frac{\Gamma \Rightarrow \Delta, \varphi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}\ (\vee R_1) \qquad \frac{\Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \vee \psi}\ (\vee R_2)$$

$$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \psi, \Gamma \Rightarrow \Delta}{\varphi \to \psi, \Gamma \Rightarrow \Delta}\ (\to L) \qquad \frac{\varphi, \Gamma \Rightarrow \Delta, \psi}{\Gamma \Rightarrow \Delta, \varphi \to \psi}\ (\to R)$$

$$\frac{\Gamma \Rightarrow \Delta, \varphi}{\neg\varphi, \Gamma \Rightarrow \Delta}\ (\neg L) \qquad \frac{\varphi, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\varphi}\ (\neg R)$$

$$\frac{\varphi\left\{\frac{t}{x}\right\}, \Gamma \Rightarrow \Delta}{\forall x\varphi, \Gamma \Rightarrow \Delta}\ (\forall L) \qquad \frac{\Gamma \Rightarrow \Delta, \varphi\left\{\frac{y}{x}\right\}}{\Gamma \Rightarrow \Delta, \forall x\varphi}\ (\forall R)^*$$

$$\frac{\varphi\left\{\frac{y}{x}\right\}, \Gamma \Rightarrow \Delta}{\exists x\varphi, \Gamma \Rightarrow \Delta}\ (\exists L)^* \qquad \frac{\Gamma \Rightarrow \Delta, \varphi\left\{\frac{t}{x}\right\}}{\Gamma \Rightarrow \Delta, \exists x\varphi}\ (\exists R)$$

The System LK [Gentzen, '34]

$$\frac{\Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\,(wkL) \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \varphi}\,(wkR)$$

$$\frac{\varphi, \varphi, \Gamma \Rightarrow \Delta}{\varphi, \Gamma \Rightarrow \Delta}\,(cntL) \qquad \frac{\Gamma \Rightarrow \Delta, \varphi, \varphi}{\Gamma \Rightarrow \Delta, \varphi}\,(cntR)$$

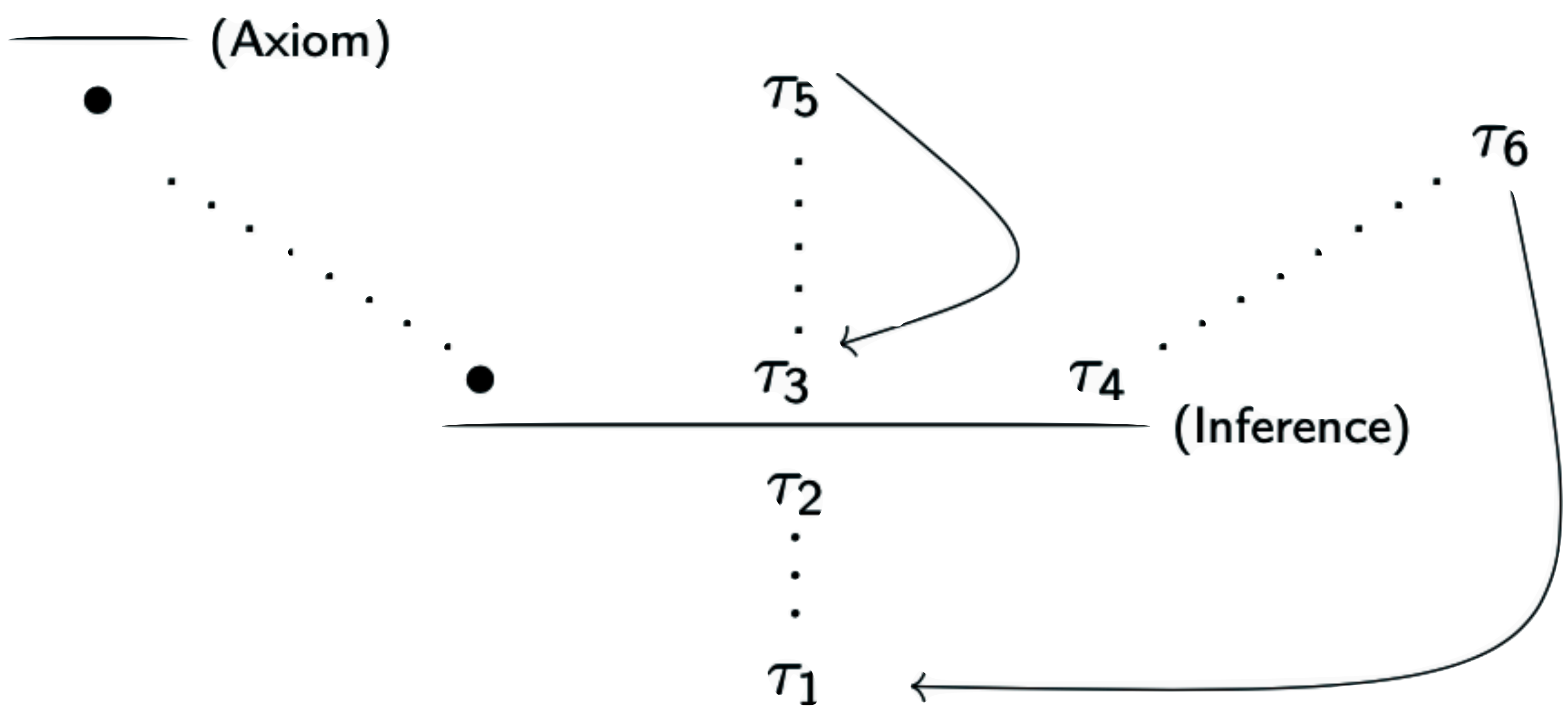
$$\frac{\Gamma \Rightarrow \Delta, \varphi \quad \varphi, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}\,(cut) \qquad \frac{\Gamma \Rightarrow \Delta}{\Gamma\left\{\frac{\vec{s}}{\vec{x}}\right\} \Rightarrow \Delta\left\{\frac{\vec{s}}{\vec{x}}\right\}}\,(sub)$$

$$\frac{}{\varphi \Rightarrow \varphi}\,(id)$$

$$\frac{\Gamma \Rightarrow \Delta, s = t \quad \Gamma \Rightarrow \Delta, \varphi\left\{\frac{s}{x}\right\}}{\Gamma \Rightarrow \Delta, \varphi\left\{\frac{t}{x}\right\}}\,(eq) \qquad \frac{}{\Rightarrow t = t}\,(eq)$$

Cyclic Reasoning

Cyclic Proofs



A cyclic pre-proof is a derivation tree with a backlink from each open leaf ("bud") to an identical "companion".

Cyclic Proof?

$$\dfrac{\dfrac{\Rightarrow 0=1}{\Rightarrow 0=1,\ 0=1}\ (\mathrm{wkR})}{\Rightarrow 0=1}\ (\mathrm{cntR})$$

"All opinions are not equal. Some are a very great deal more robust, sophisticated and well supported in logic and argument than others"

-Douglas Adams

Is this a valid pre-proof?

The cycle does not make any "progress"

How can we rule out such pre-proofs?

Infinite Descent

"Because the ordinary methods now in the books were insufficient for demonstrating such difficult propositions, I finally found a totally unique route for arriving at them . . . which I called infinite descent . . ."

–Pierre de Fermat, 1659

Theorem: $\sqrt{2}$ is not rational

Proof: Suppose for contradiction that $\sqrt{2} = \frac{x}{y}$ for $x, y \in \mathbb{N}$. Then, $x^2 = 2y^2$.

Consequently $x(x-y) = y(2y-x)$, so that: $\frac{2y-x}{x-y} = \frac{x}{y} = \sqrt{2}$

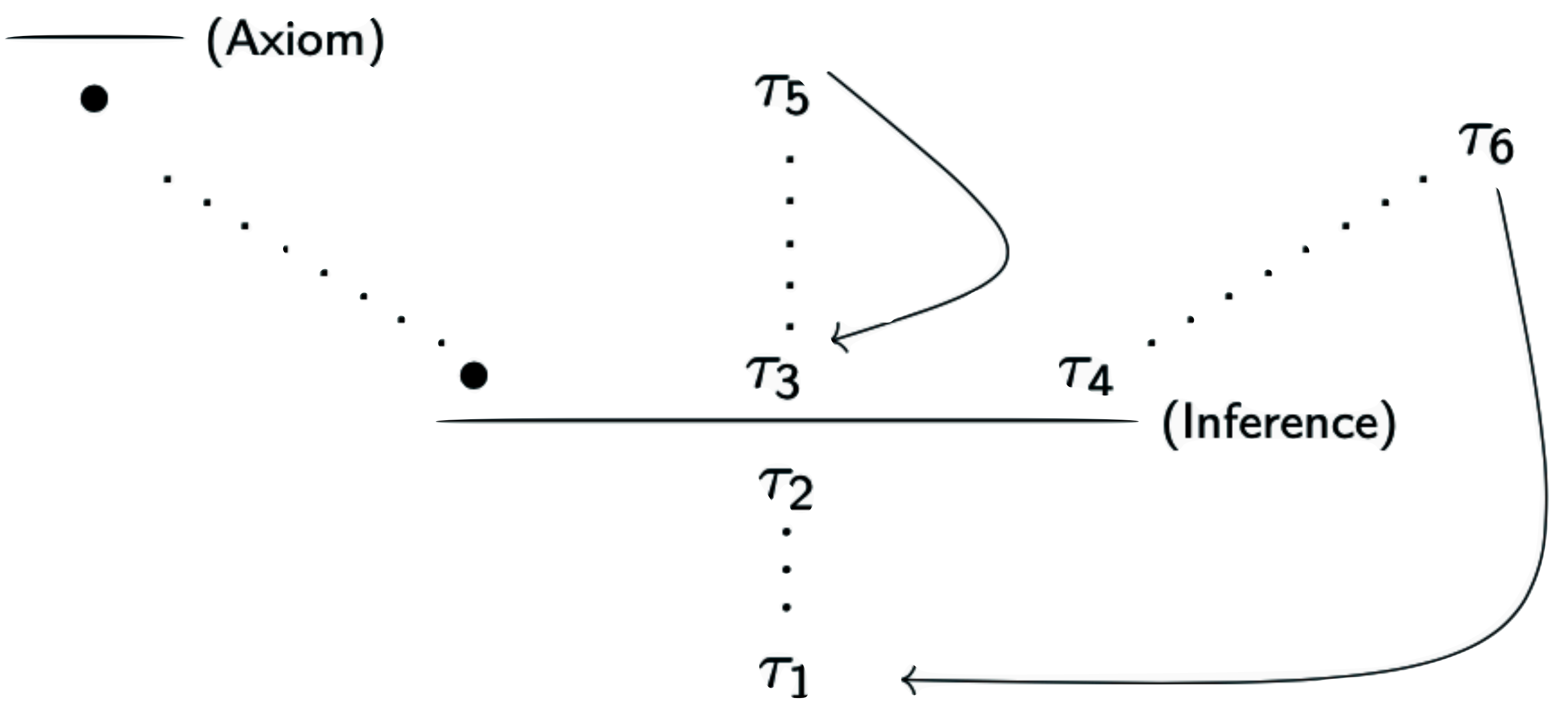
Define: $x' = 2y - x$ and $y' = x - y$. Then, $\sqrt{2} = \frac{x'}{y'}$.

Since $y < \sqrt{2}y = x < 2y$, and so $0 < x - y = y' < y$.

But then we have $x', y' \in \mathbb{N}$ such that $\sqrt{2} = \frac{x'}{y'}$ and $y' < y$.

Infinite descent from y

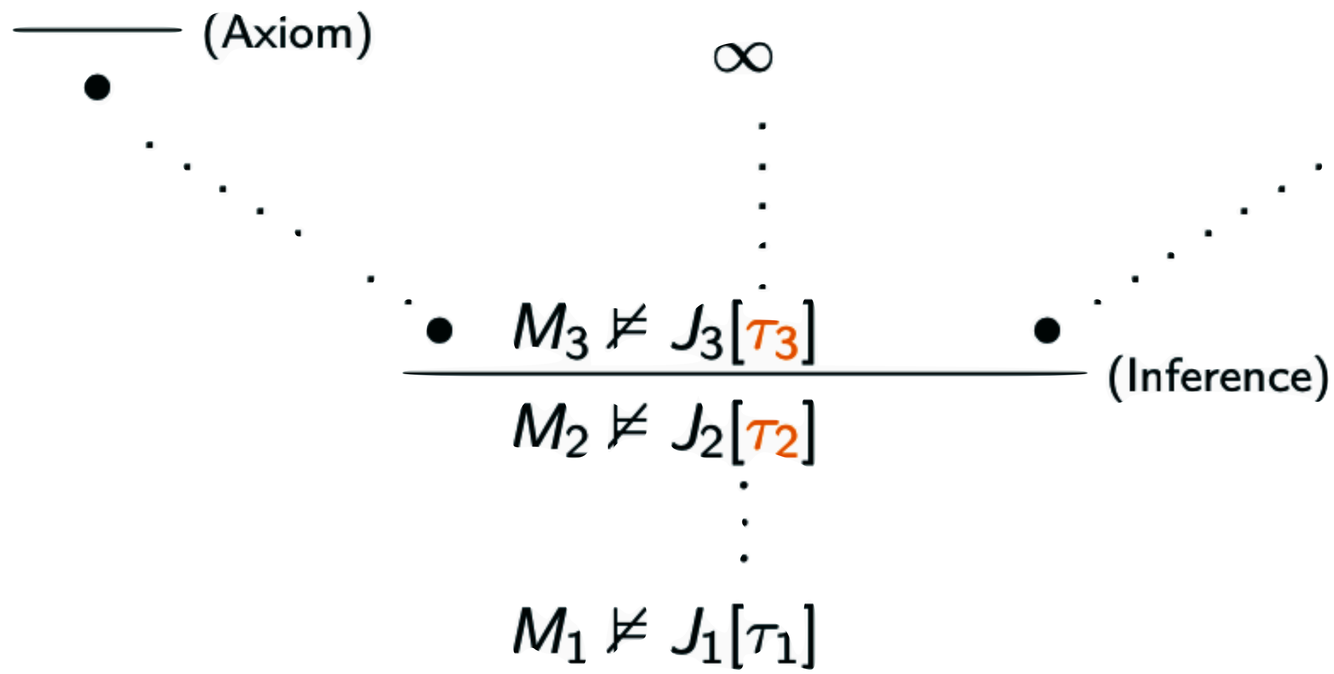
Soundness Criteria



A cyclic proof =
A pre-proof
+
Soundness condition
(for every infinite path there is an infinitely progressing trace along some tail)

- We trace syntactic elements τ (terms/formulas) through judgements
  - At certain points, there is a notion of 'progression'
- Each infinite path must admit some infinite descent
- The Infinite Descent condition is an ω-regular property (i.e decidable)

Soundness via Infinite Descent



- Assume for contradiction that the conclusion is invalid
  - Local soundness ⇒ counter-models M_1, M_2, M_3, ...
- We demonstrate a mapping into well-founded (D,<) s.t.
  - $[[M_1]]_{J_1[\tau_1]} \leq [[M_2]]_{J_2[\tau_2]} \leq [[M_3]]_{J_3[\tau_3]} \leq \ldots$
  - $[[M_2]]_{J_2[\tau_2]} < [[M_3]]_{J_3[\tau_3]}$ for progression points
- Infinite Descent condition ⇒ infinitely descending chain in D!

Proof Example

Consider these inductive definitions of predicates N, E, O:

$$\Rightarrow N0 \qquad\qquad Nx \Rightarrow Nsx$$

$$\Rightarrow E0 \qquad\qquad Ex \Rightarrow Osx \qquad\qquad Ox \Rightarrow Esx$$

These definitions generate case-split rules, e.g., for E:

$$\dfrac{\Gamma, t = 0 \Rightarrow \Delta \qquad \Gamma, t = sx, \boxed{Ox} \Rightarrow \Delta}{\Gamma, \boxed{Et} \Rightarrow \Delta}$$

$$\dfrac{\dfrac{\dfrac{}{\Rightarrow \mathsf{N}\,\mathbf{0}}\,(\mathsf{N\,R_1})}{x = \mathbf{0} \Rightarrow \mathsf{N}\,x}\,(=\mathsf{L}) \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathsf{E}\,x \Rightarrow \mathsf{N}\,x}{\mathsf{E}\,z \Rightarrow \mathsf{N}\,z}\,(\mathsf{Subst})}{\mathsf{E}\,z \Rightarrow \mathsf{N}\,\mathbf{s}\,z}\,(\mathsf{N\,R_2})}{y = \mathbf{s}\,z, \mathsf{E}\,z \Rightarrow \mathsf{N}\,y}\,(=\mathsf{L})}{\mathsf{O}\,y \Rightarrow \mathsf{N}\,y}\,(\mathsf{Case\ O})}{\mathsf{O}\,y \Rightarrow \mathsf{N}\,\mathbf{s}\,y}\,(\mathsf{N\,R_2})}{x = \mathbf{s}\,y, \mathsf{O}\,y \Rightarrow \mathsf{N}\,x}\,(=\mathsf{L})}{\mathsf{E}\,x \Rightarrow \mathsf{N}\,x}\,(\mathsf{Case\ E})$$

Open Questions

Can we prove more?

- In general, cyclic systems subsume explicit system
- But are they really stronger?

- Does the translation between the two forms preserves important patterns (e.g. modularity)?

Can we prove better?

- Elegance
- Automation/proof search
- Separating termination from correctness
- Inductive invariants

Can we check soundness better?

- Traditionally managed by encoding it as the inclusion between two Büchi automata
  - exponential blow-up of execution time on the number of nodes
  - lacks transparency and flexibility

- Better alternative intrinsic criteria which operate directly on the proof tree
  - improved complexity
  - direct explanation of why the condition holds/fails

Can we get more automated support?

- Provers (automated/semi-automated) currently offer little or no support for cyclic reasoning
    - exceptions: Cyclist
- Major verification efforts are missing the great potential of cyclic reasoning for lighter, more legible and more automated proofs.

"Proving theorems is not for the mathematicians anymore: with theorem provers, it's now a job for the hacker."
— Martin Rinard