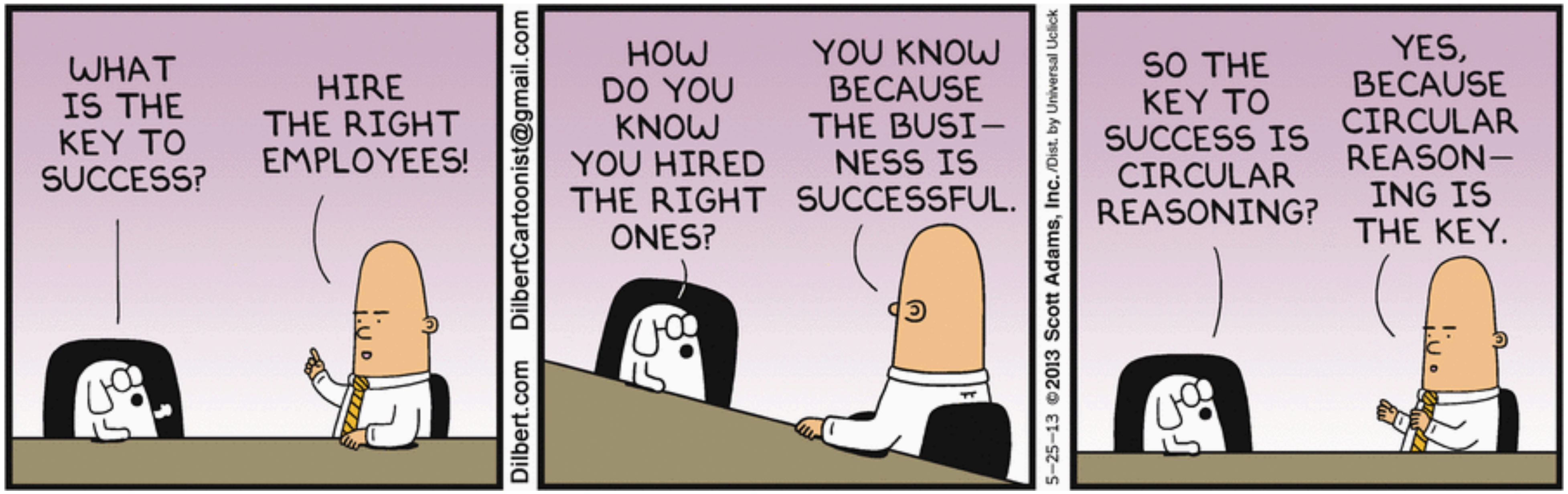
Non-Well-Founded Proofs and Non-Well-Founded Research

Liron Cohen



LMW@LICS 2025

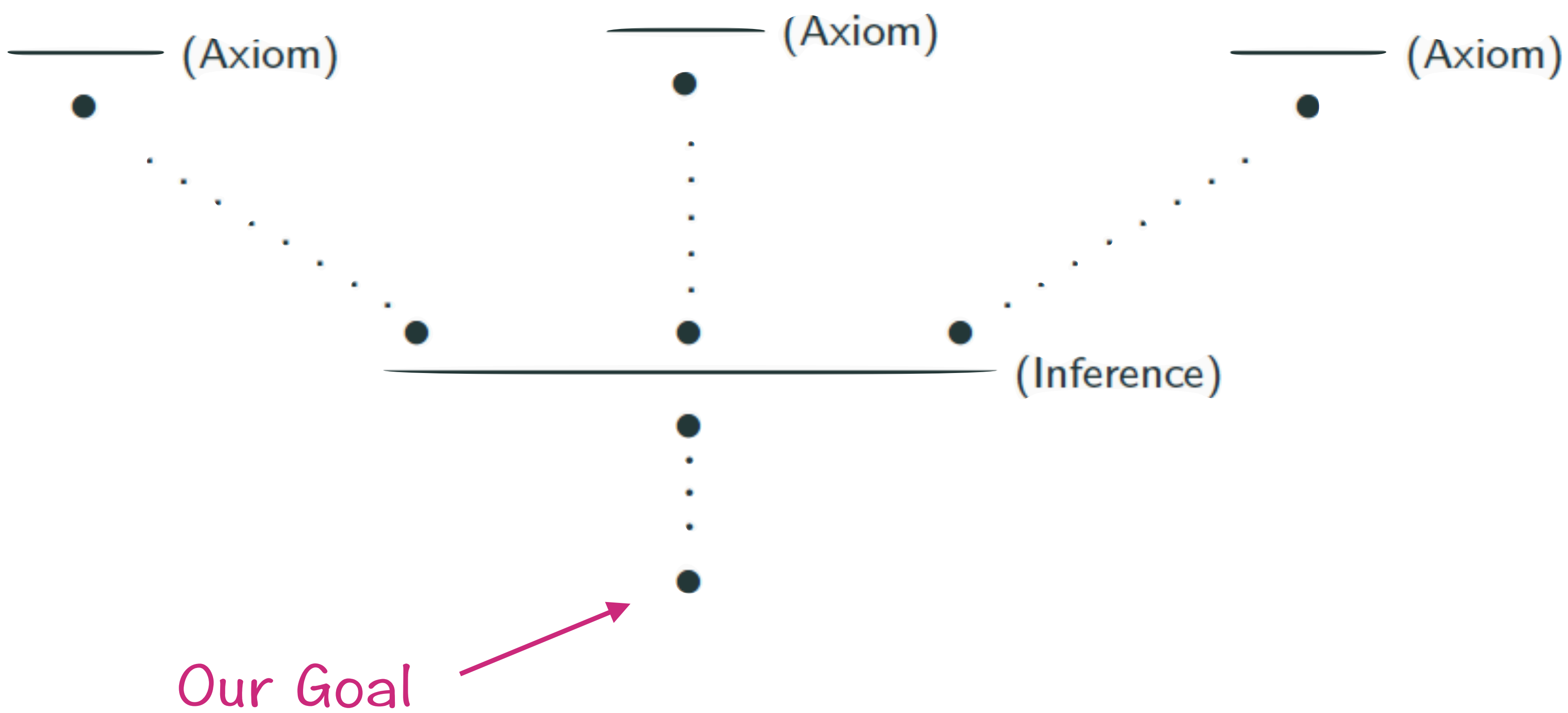
cliron@bgu.ac.il

Who am I ?

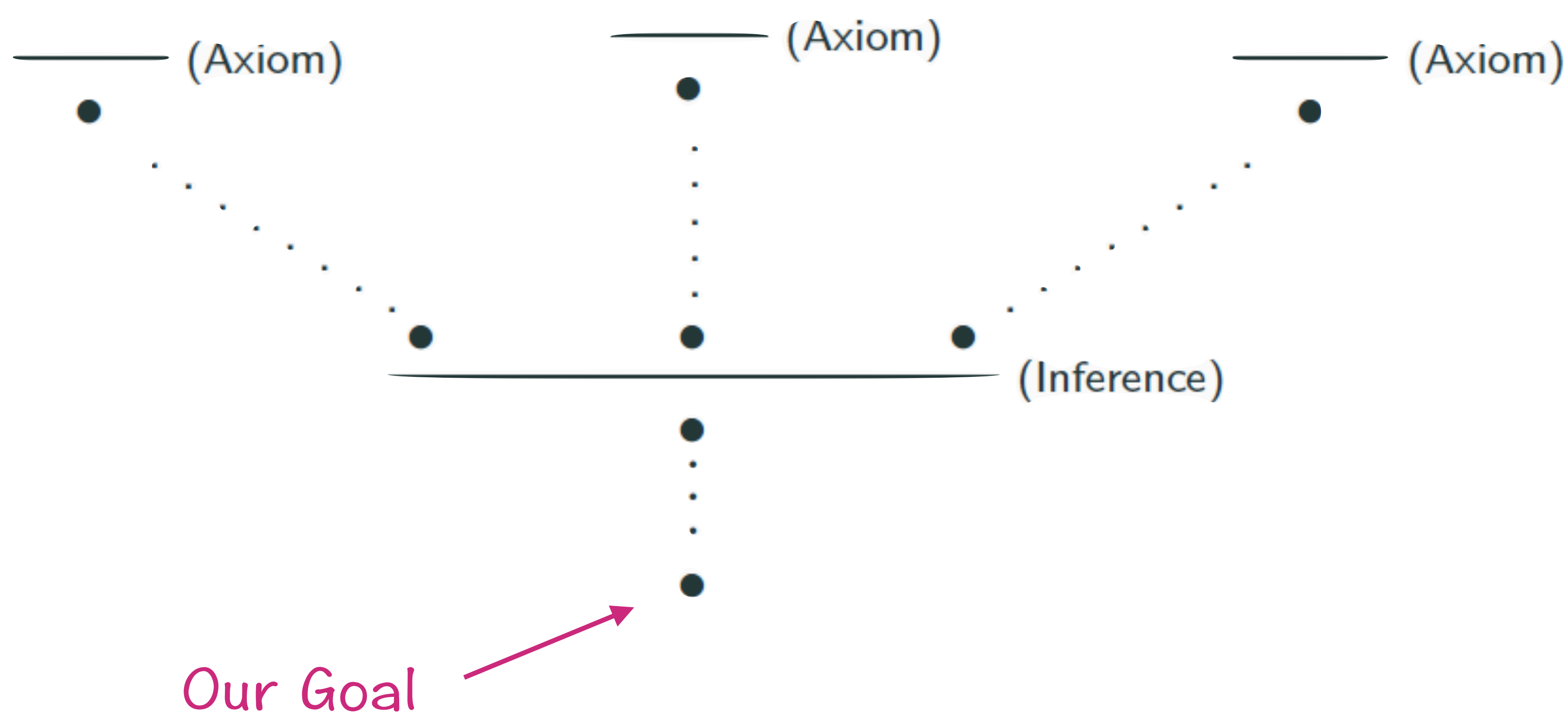
Some research interests:

- Type systems and computational models
- Theorem proving and automated reasoning
- Proof theory
- Computational mathematics

Well-Founded Proofs

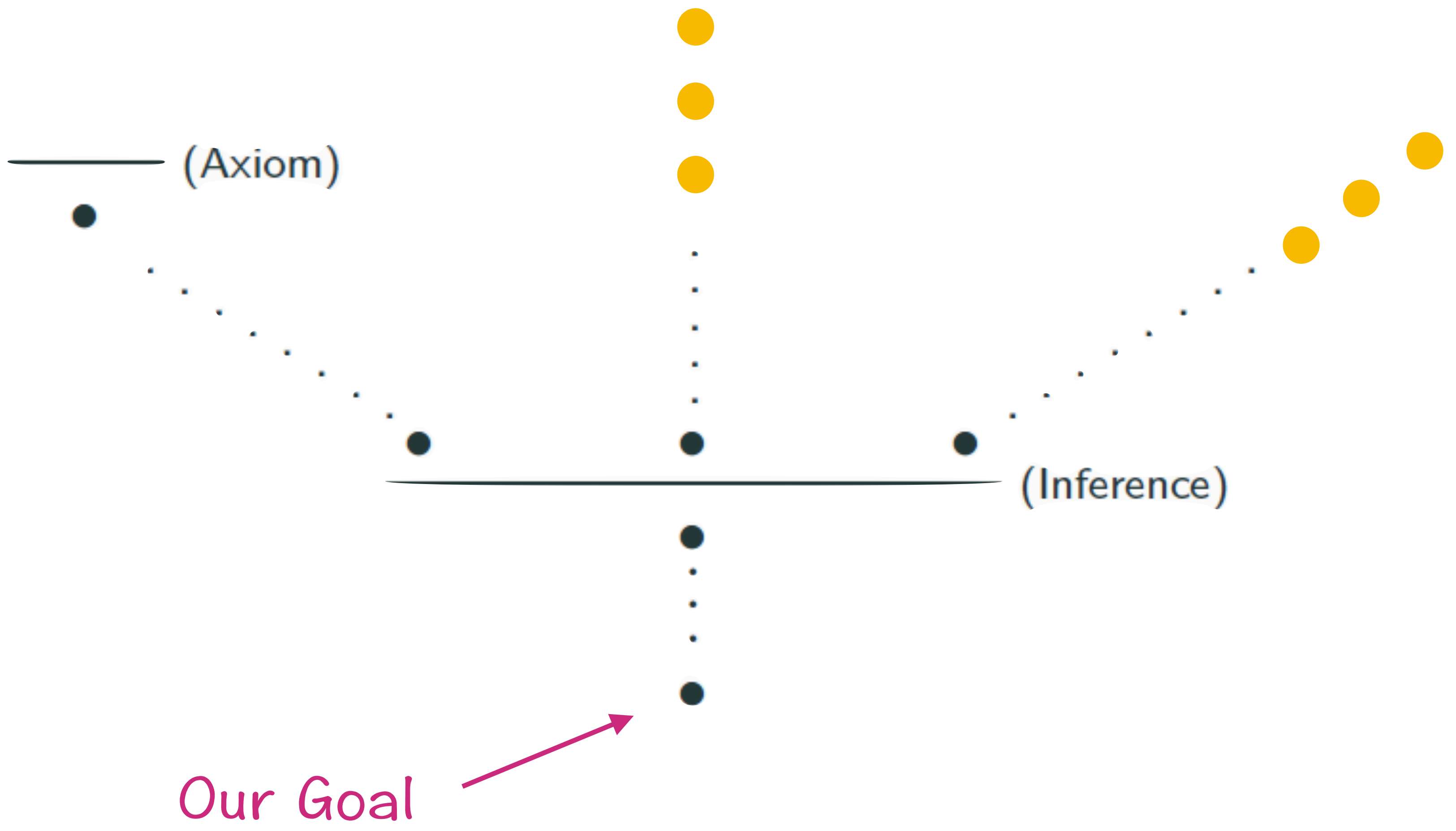


Well-Founded Proofs

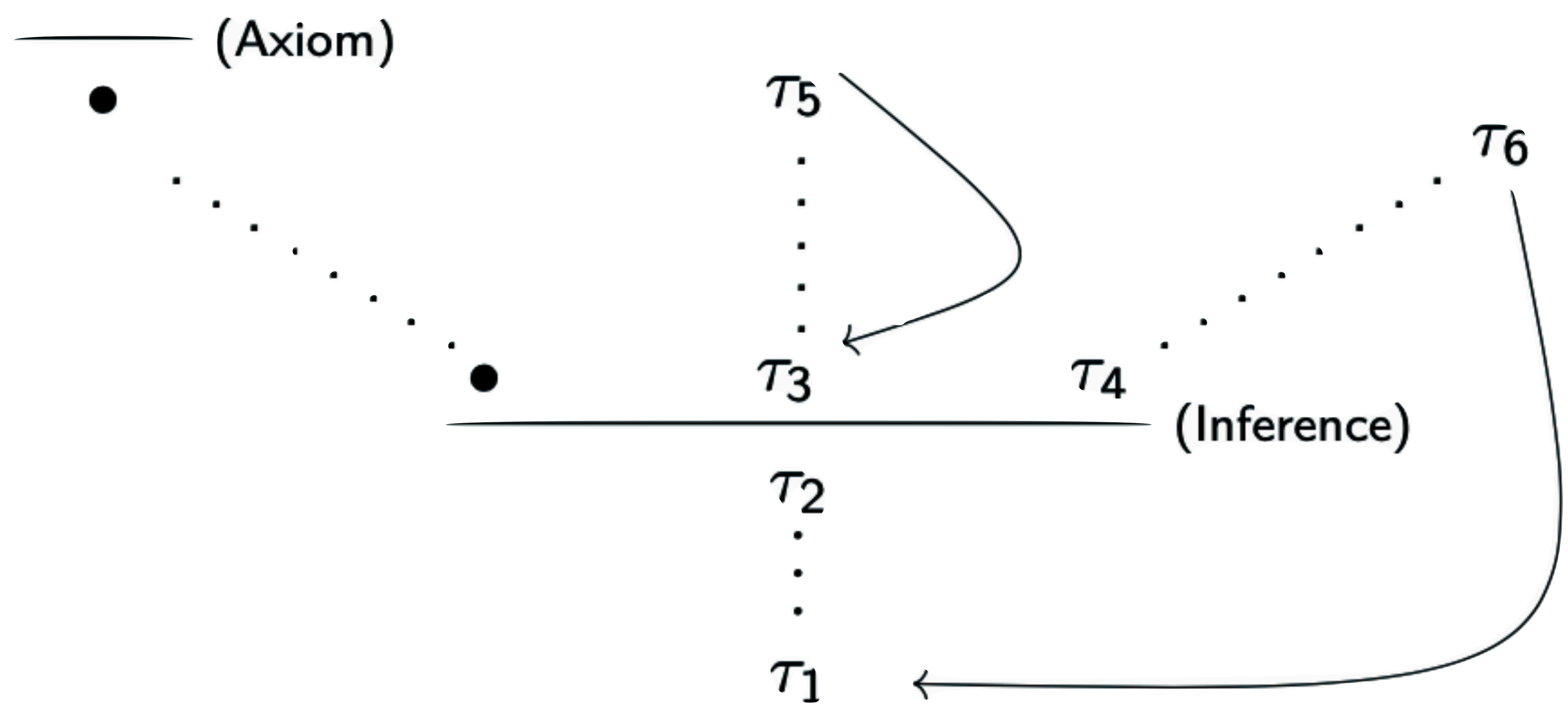


Soundness: If the axioms are sound and every inference rule is sound, then every proof is sound.

Non-Well-Founded Proofs

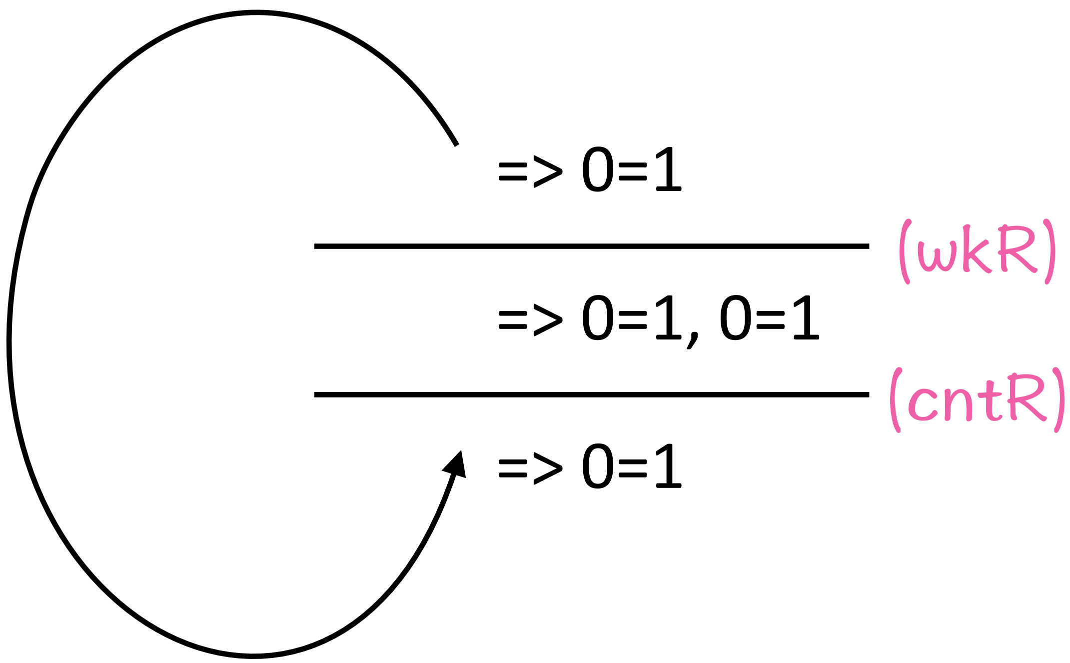


Non-Well-Founded Proofs



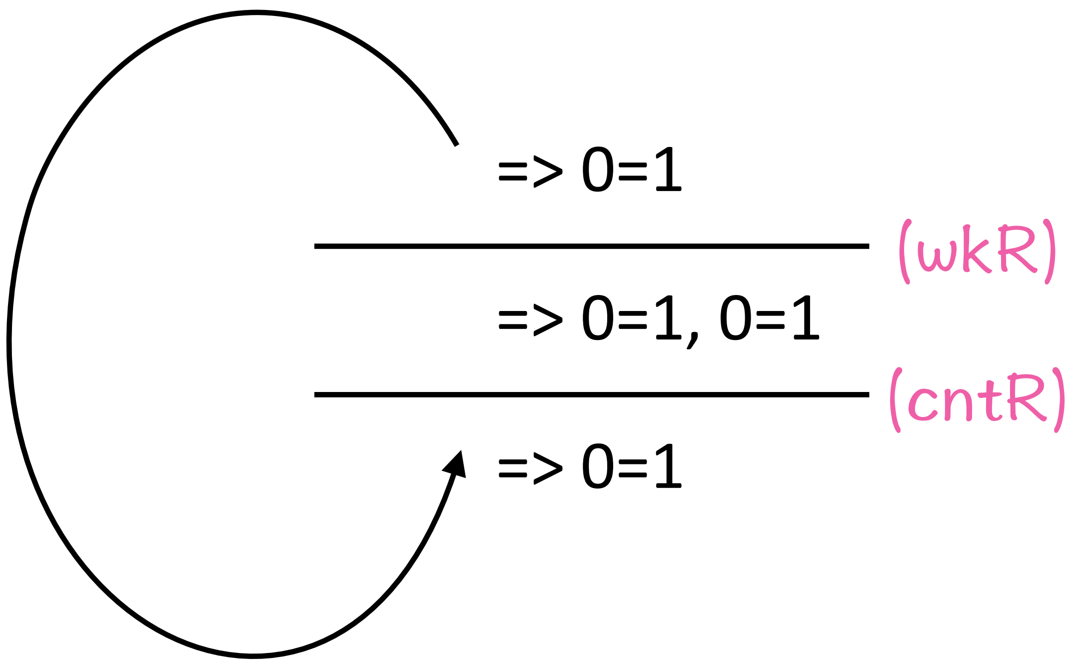
A cyclic pre-proof is a derivation tree with a backlink from each open leaf ("bud") to an identical "companion".

Cyclic Proof?



Is this a valid pre-proof?

Cyclic Proof?



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

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

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, $x^2 = 2y^2$.

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: $\frac{2y-x}{x-y} = \frac{x}{y} = \sqrt{2}$

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, $\sqrt{2} = \frac{x'}{y'}$.

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 $0 < x - y = y' < y$.

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

"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: $\frac{2y-x}{x-y} = \frac{x}{y} = \sqrt{2}$

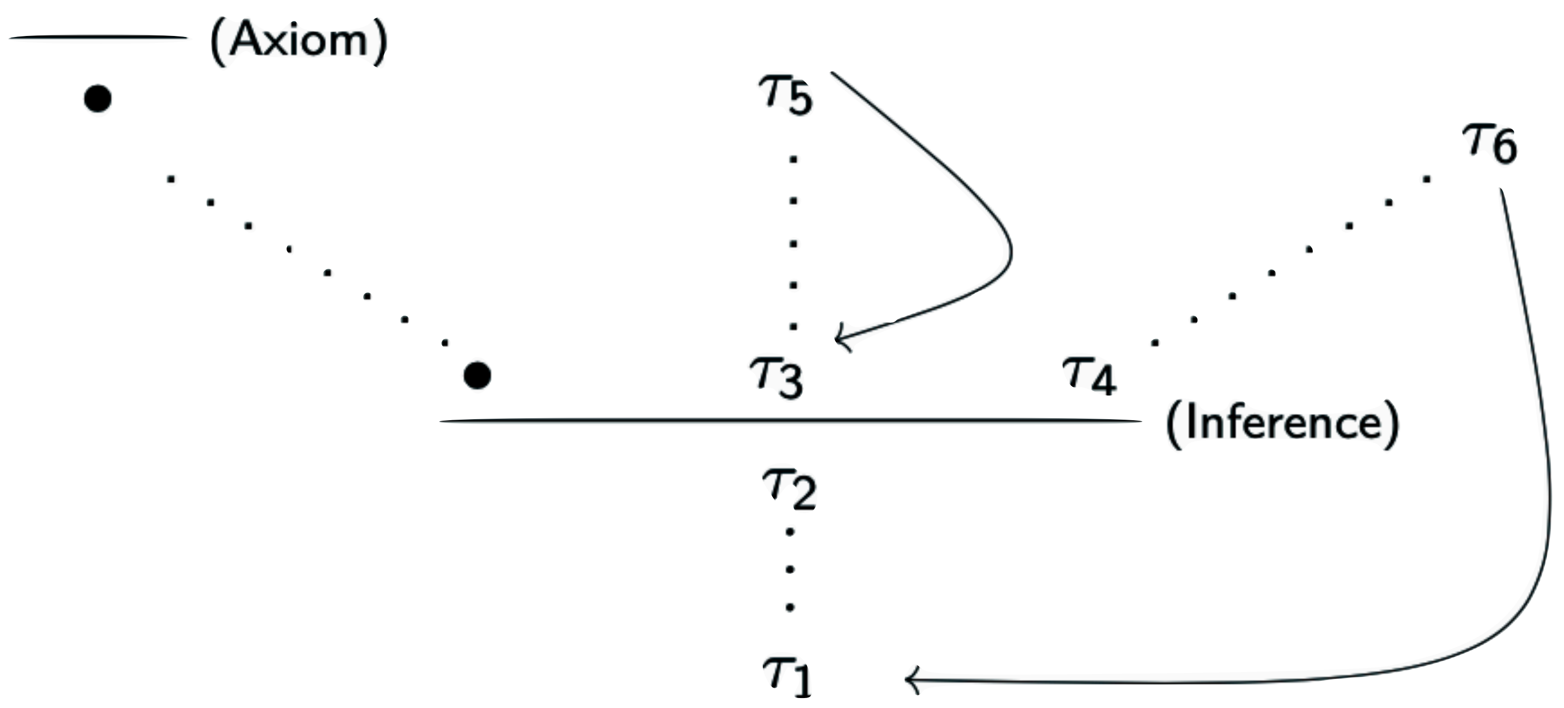
Define: $x' = 2y - x$ and $y' = x - y$. Then, $\sqrt{2} = \frac{x'}{y'}$.

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

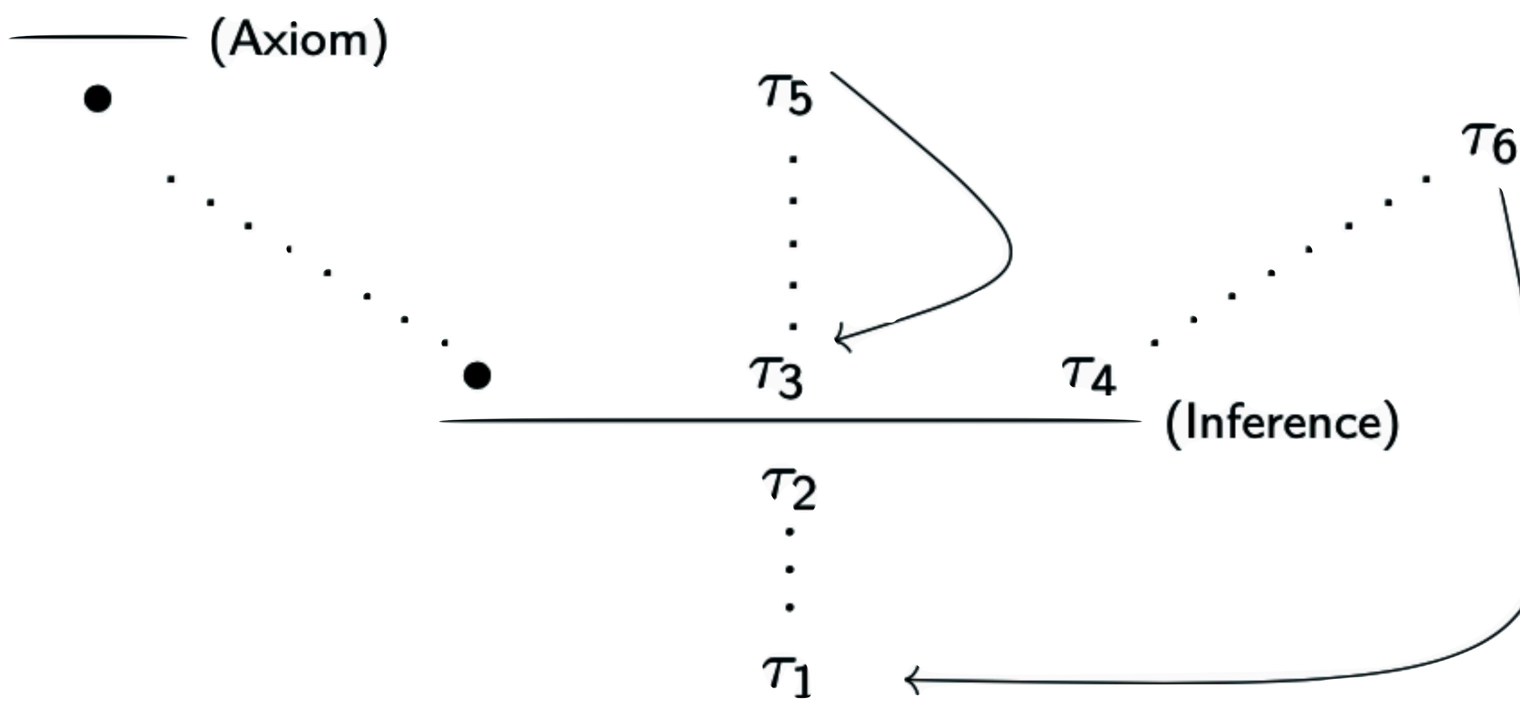
But then we have $x', y' \in \mathbb{N}$ such that $\sqrt{2} = \frac{x'}{y'}$ and $y' < y$.

Infinite descent from y

Soundness Criteria

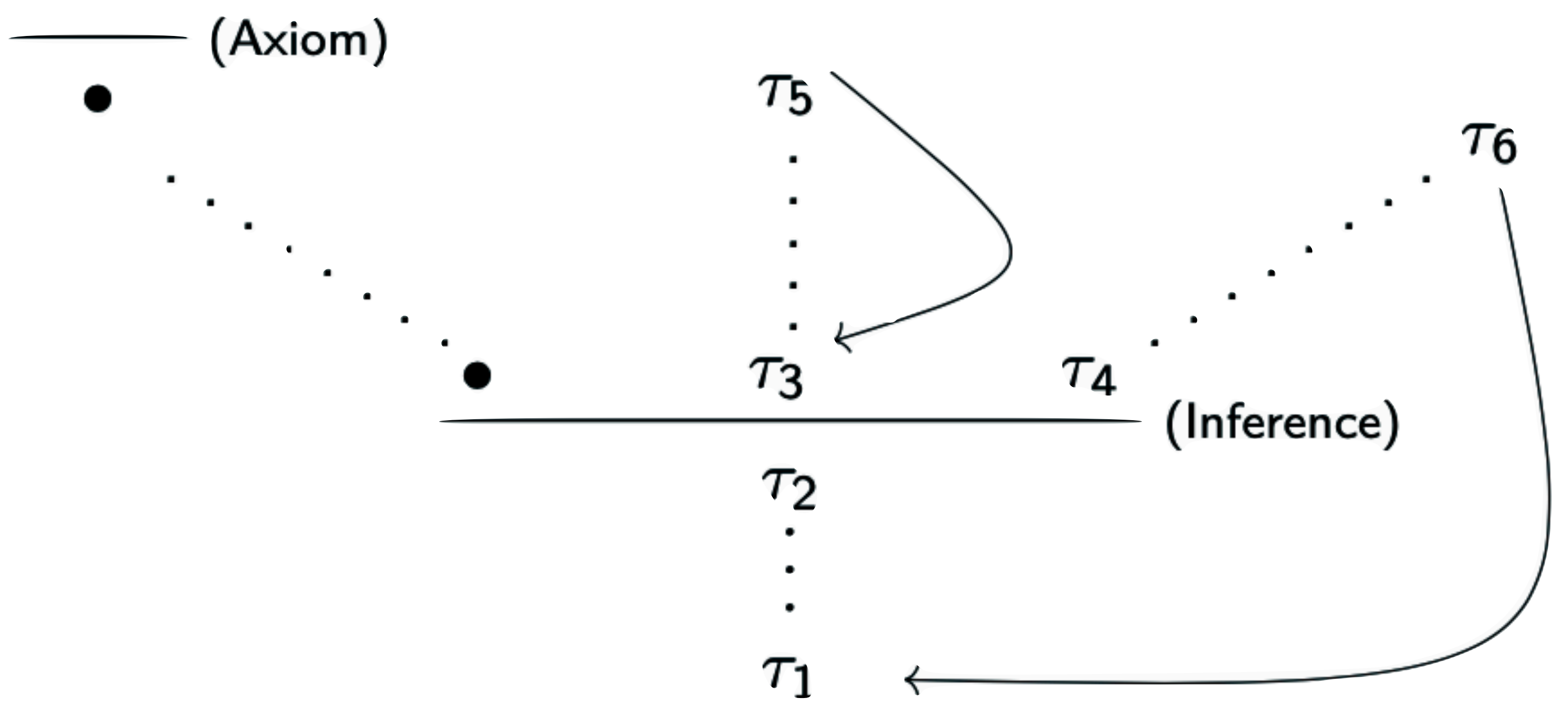


Soundness Criteria



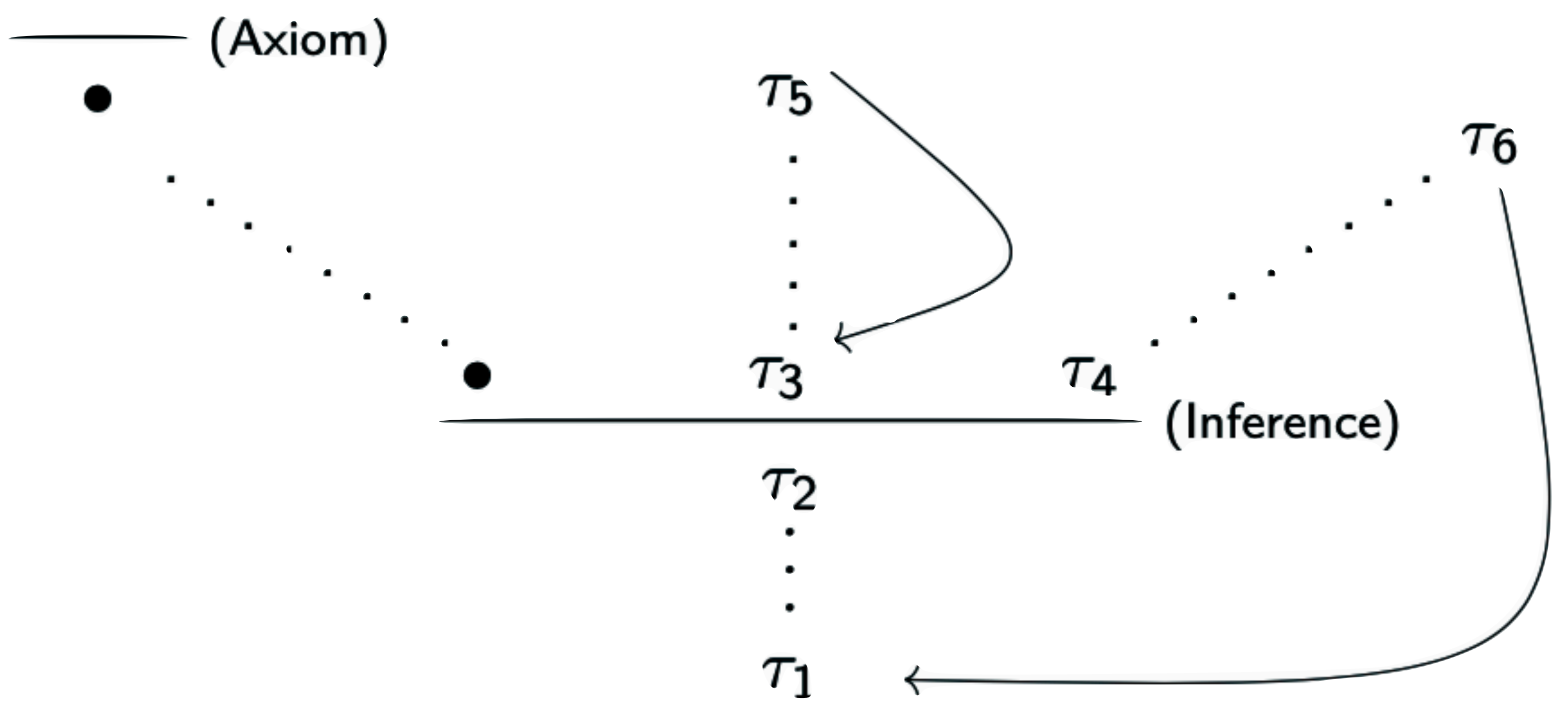
- We trace syntactic elements τ (terms/formulas) through judgements
  - At certain points, there is a notion of 'progression'
- Each infinite path must admit some infinite descent

Soundness Criteria



- 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 Criteria



A cyclic proof =
A pre-proof
+
Soundness condition
(every infinite path has 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)

Proof Example

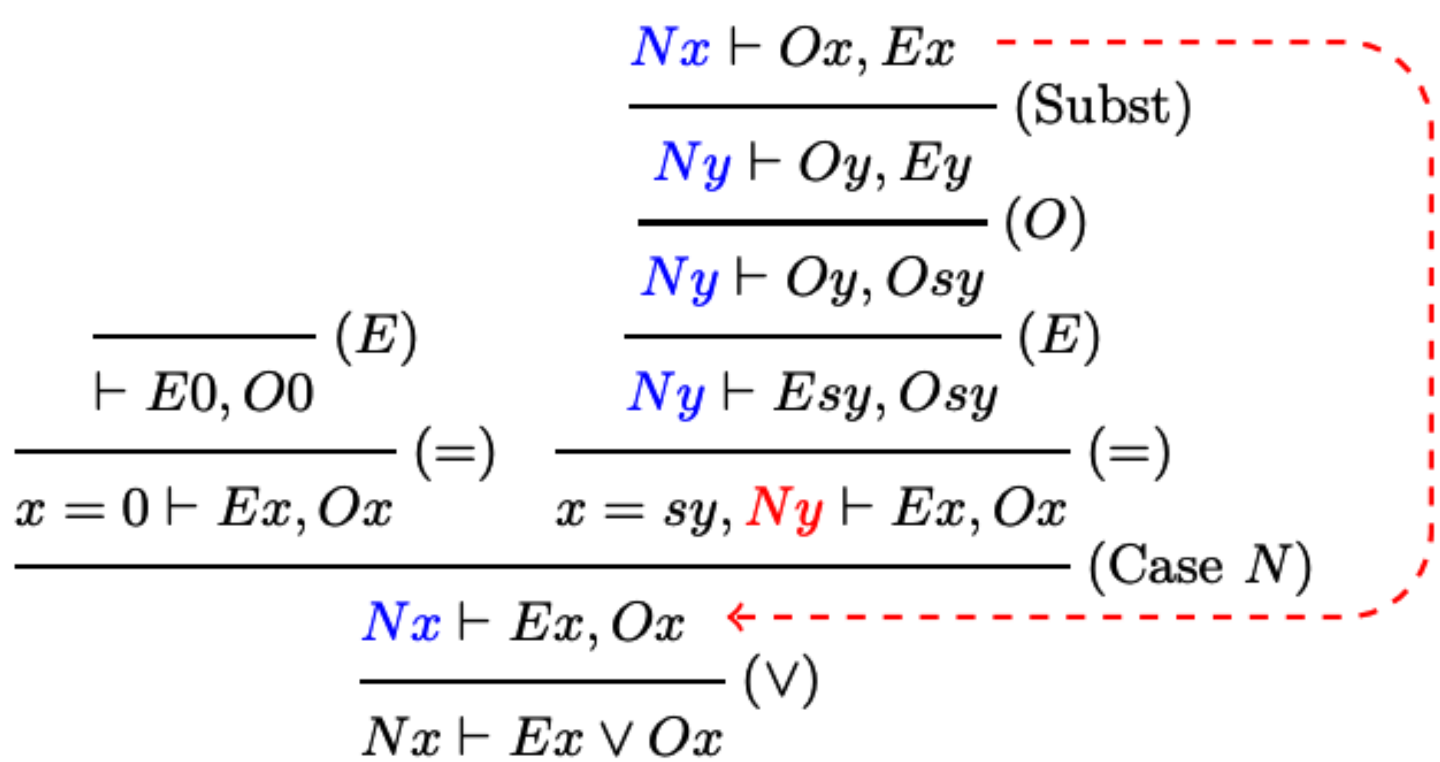
Consider these inductive definitions of predicates N, E, O:

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

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

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

$$\frac{\Gamma, t = 0 \Rightarrow \Delta \qquad \Gamma, t = sx, Nx \Rightarrow \Delta}{\Gamma, Nt \Rightarrow \Delta}$$



Some Logics with Cyclic Proof Systems

- μ-calculus (modal, first-order)
- Temporal logic (CTL, LTL,. . .)
- First-order logic with ind. definitions
- Transitive closure logic
- Separation logic with ind. definitions
- Hoare logic and variants (e.g. termination)
- Linear logic with fixed points
- Modal logic (of certain kinds)
- Kleene algebras
- Combinations of the above…

"contrariwise,
if it was so, it might be,
and if it were so, it would be;
but as it isn't, it ain't.
That's logic!"

-Tweedledee (Lewis carroll)

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 Infinite Descent efficiently?

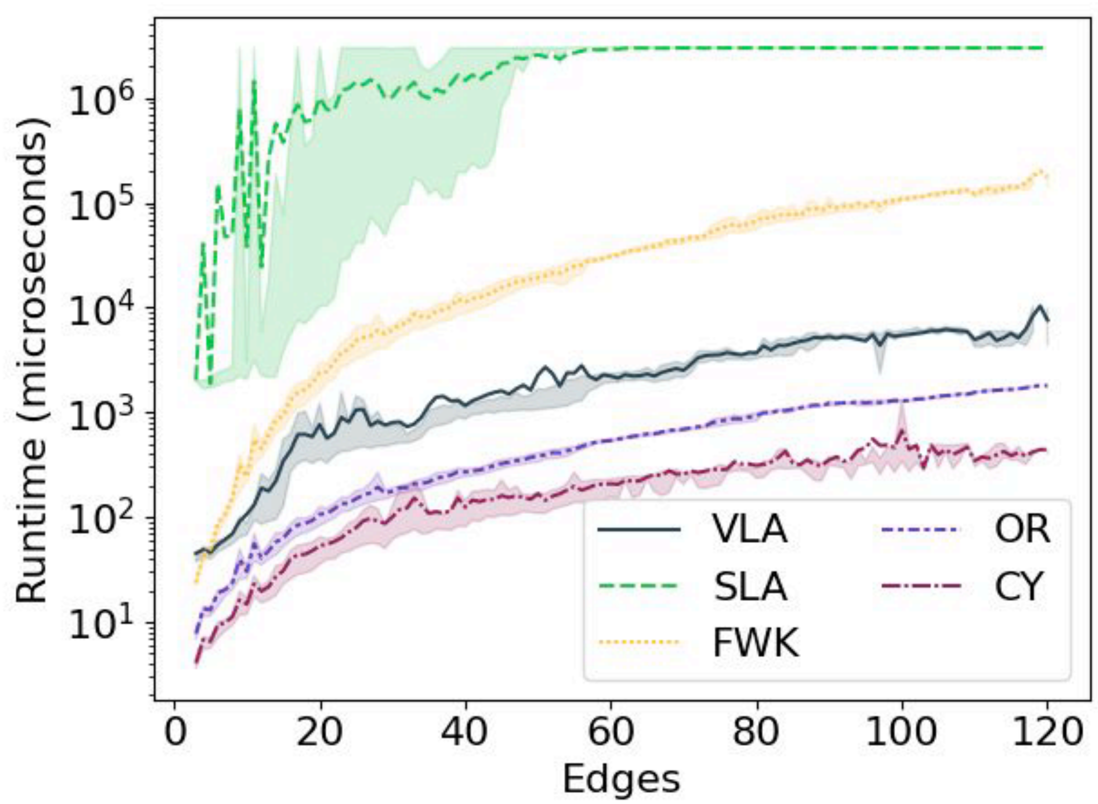
- Checking Infinite Descent is PSPACE-complete
- There are two classes of algorithms in the literature:
  - Automata-theoretic: Checks inclusion between ω-automata recognizing paths
  - Ramsey-theoretic (relation-based): Compute compositions of sloped relations along all finite paths

	Algorithm	Time Complexity Upper Bound
Automata-theoretic	VLA	$\mathcal{O}(n^5 \cdot w^2 \cdot 2^{2nw \log(2nw)})$
	SLA	$\mathcal{O}(n^2 \cdot w \cdot \min(n^4, 3^{2w^2}) \cdot 2^{2w \log(2w)})$
Ramsey-theoretic	FWK	$\mathcal{O}(n \cdot w^4 \cdot 3^{3w^2} + n^3 \cdot w^4 \cdot 3^{2w^2})$
	OR	$\mathcal{O}(n^3 \cdot w^4 \cdot 3^{2w^2})$

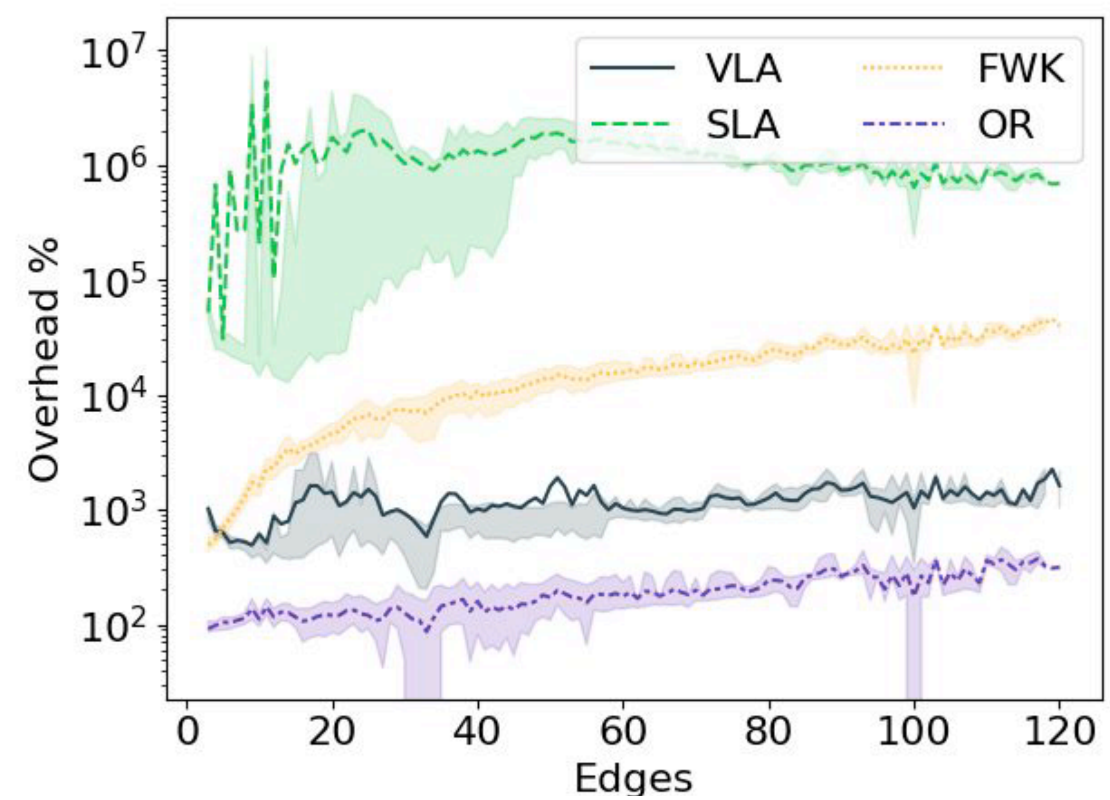
Can we check Infinite Descent efficiently, if we forgo completeness?

YES!

The tool CYCLONE implements a serial pipeline of sound heuristics, defaulting to a complete method



Average runtime of methods, aggregated by #edges



Average % overhead of complete methods compared to CYCLONE, aggregated by #edges

Can we get more automated support?

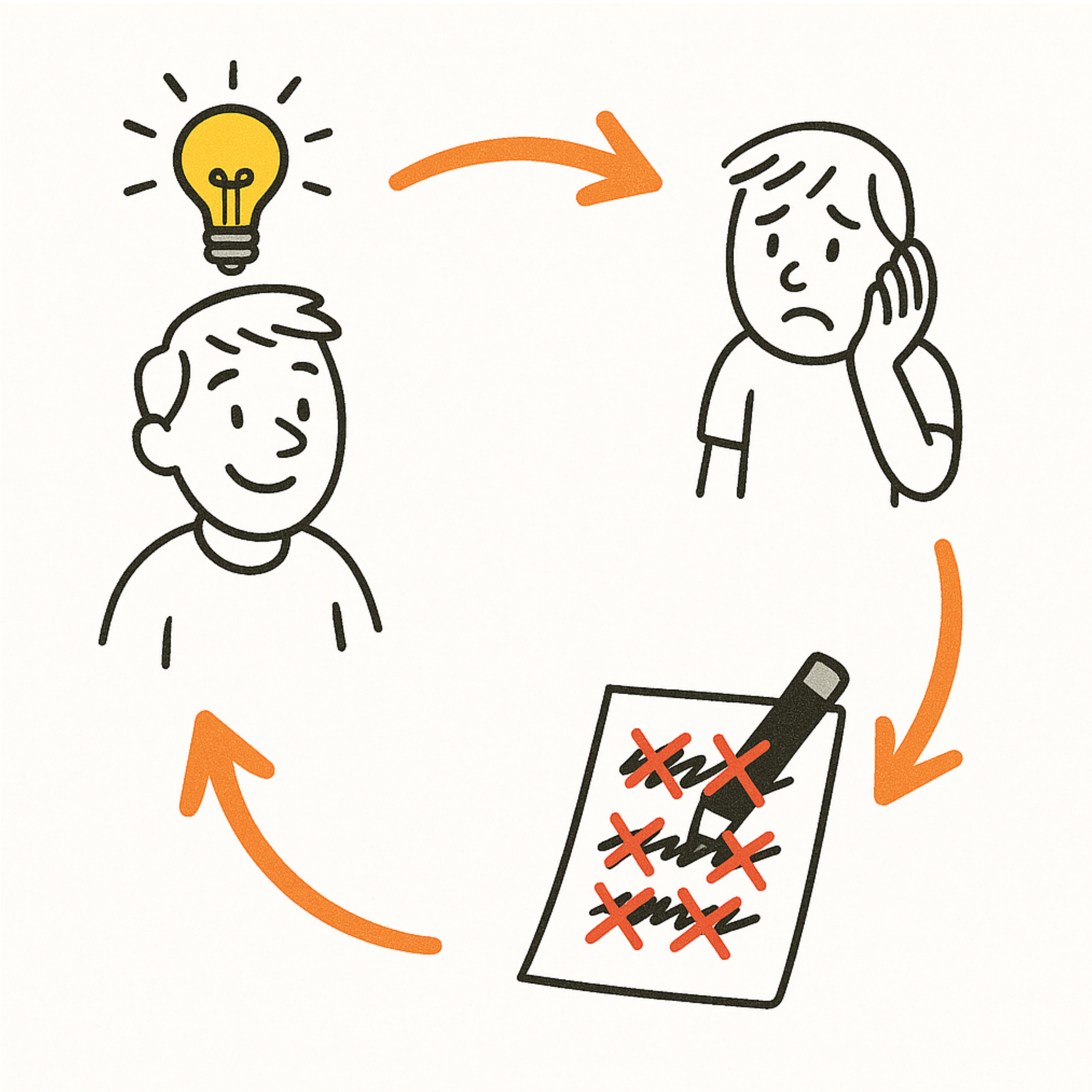
- Provers (automated/semi-automated) currently offer little or no support for cyclic reasoning
    - exceptions: Cyclist

- 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

And what about research?

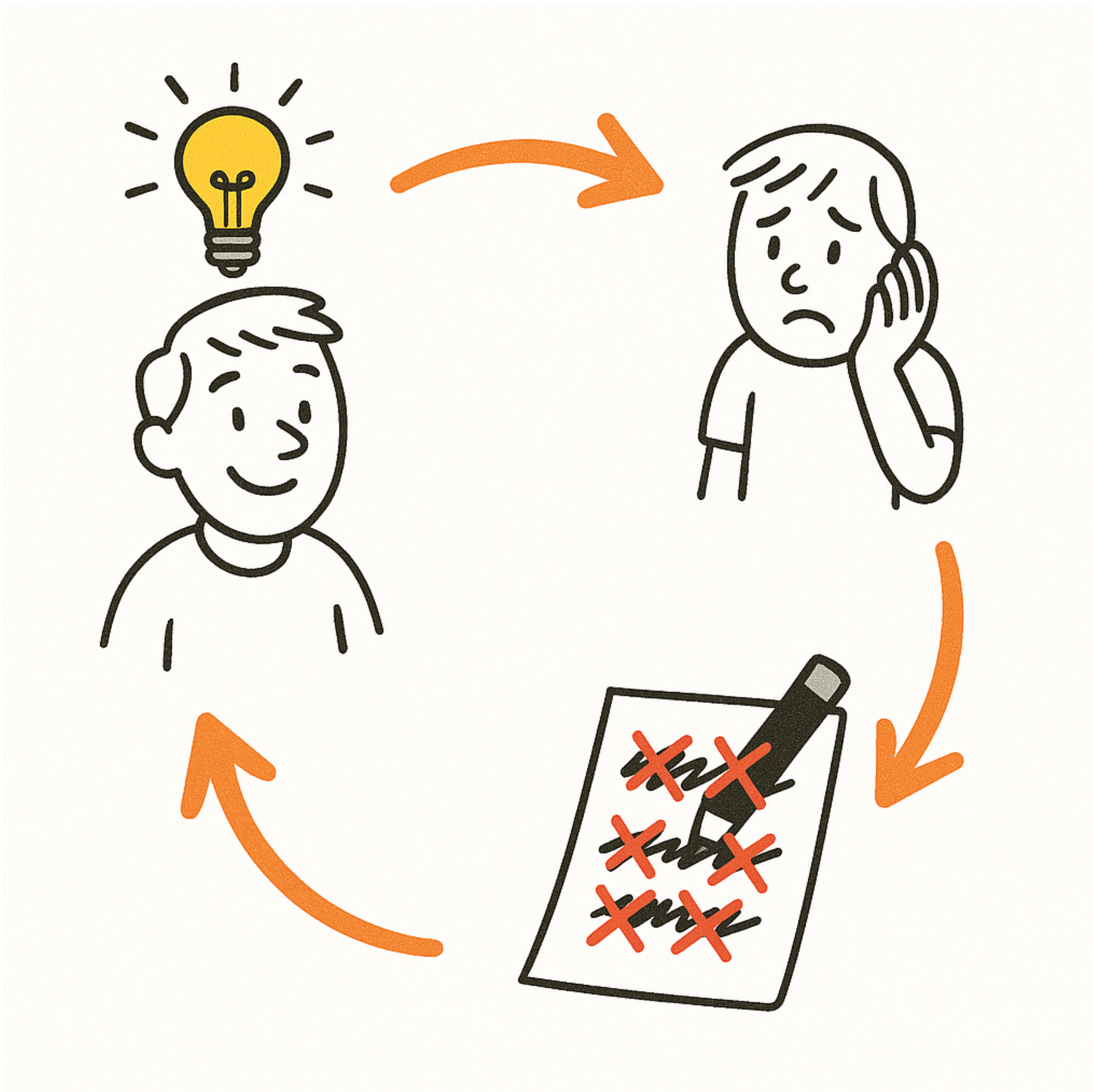
Research is Non-Well-Founded



Eventually, we publish a paper claiming we knew it all along.

Sounds Familiar?

Research is Non-Well-Founded



Eventually, we publish a paper claiming we knew it all along.

Sounds Familiar?

- We loop back to earlier ideas
- Definitions evolve
- Proof strategies change
- Goals shift

The Key is to Find your Infinite Descent!

The Key is to Find your Infinite Descent!

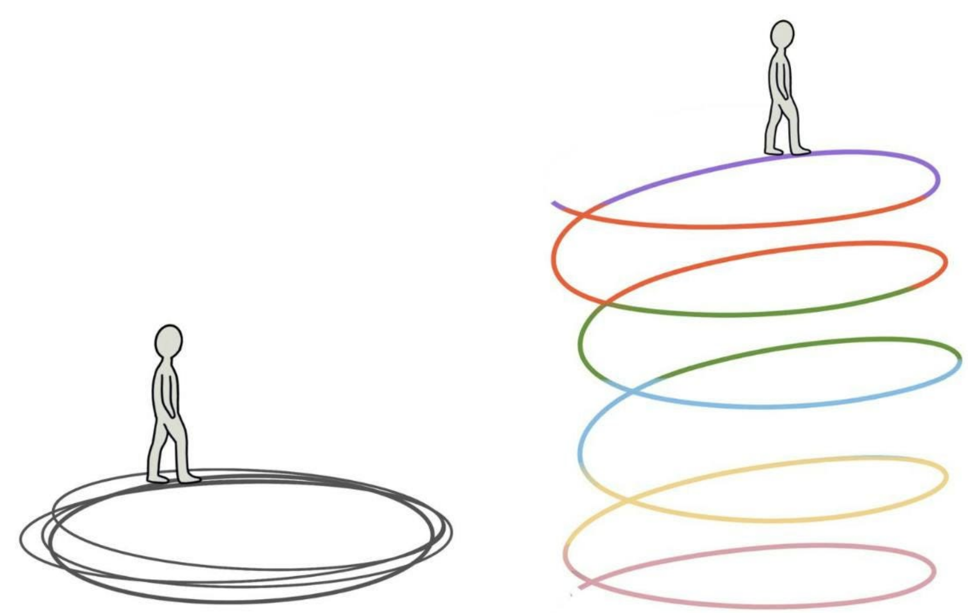
- We ensure progress through infinite descent.

The Key is to Find your Infinite Descent!

- We ensure progress through infinite descent.
- Whenever we cycle we need to make sure we have:
  - Sharpened intuitions
  - Cleaner formalisms
  - A better counterexample
  - Better questions

The Key is to Find your Infinite Descent!

- We ensure progress through infinite descent.
- Whenever we cycle we need to make sure we have:
  - Sharpened intuitions
  - Cleaner formalisms
  - A better counterexample
  - Better questions
- Remember: Non-well-founded doesn't mean unsound
- The Problem: infinite descent is a global property



So How Do We Keep Cycling?

So How Do We Keep Cycling?

- Find mentors
- Find friends
- Find collaborators
- Consult/ask for help
- People like to give advice**
- Present your work wherever you can
- Be a good citizen

So How Do We Keep Cycling?

- Find mentors
- Find friends
- Find collaborators
- Consult/ask for help
- People like to give advice**
- Present your work wherever you can
- Be a good citizen

Find something well-founded!

So How Do We Keep Cycling?

- Find mentors
- Find friends
- Find collaborators
- Consult/ask for help
- People like to give advice**
- Present your work wherever you can
- Be a good citizen

Find something well-founded!

cliron@bgu.ac.il