μHOL^{ex}, a cyclic proof system for higher-order fixed point logic

Chris Purdy, Reuben Rowe - Royal Holloway, University of London

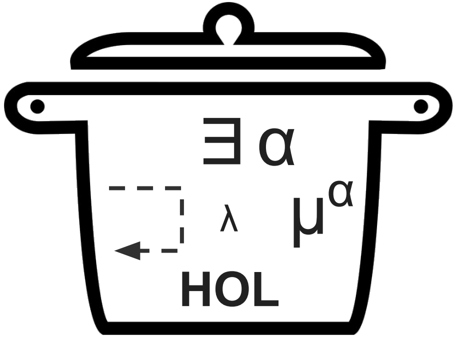
Our goal

"Develop a **cyclic** meta-theoretic basis
for a **proof assistant**."

$\mu\mathrm{HOL}^{ex}$

Higher-order

Fixed points



Cyclic deduction
system

Ordinal approximations

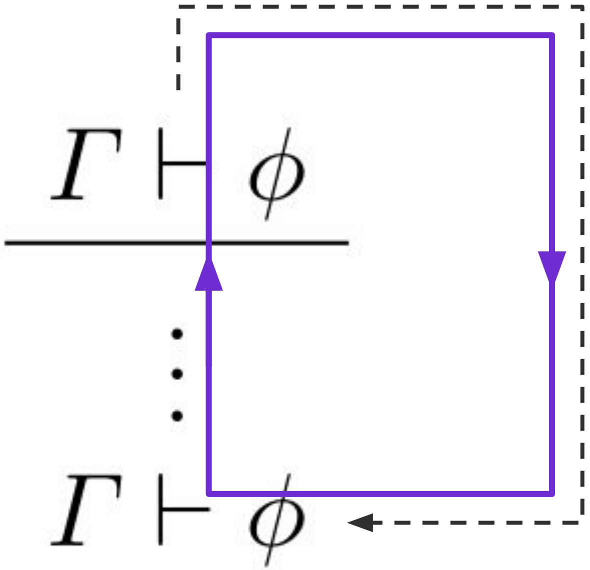
Computational interpretation

Cyclic proofs vs. finite proofs

$$\dfrac{\overline{\;\Gamma' \vdash \phi'\;}\,(\mathrm{ax})}{\begin{array}{c}\vdots \\ \Gamma \vdash \phi\end{array}}$$

In many deductive systems, proofs are **finite** derivation trees.

There must be some **progress** along each cycle - progress is specified by a **trace condition**.



Cyclic proofs are **regular non-well-founded** derivation trees.

A cyclic proof

$$\frac{}{\mathrm{Nat}(0)} \qquad \frac{\mathrm{Nat}(x)}{\mathrm{Nat}(\mathrm{succ}\ x)}$$

$$\frac{}{\mathrm{Even}(0)} \qquad \frac{\mathrm{Even}(x)}{\mathrm{Odd}(\mathrm{succ}\ x)} \qquad \frac{\mathrm{Odd}(x)}{\mathrm{Even}(\mathrm{succ}\ x)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \mathrm{Nat}(0)}}{x = 0 \vdash \mathrm{Nat}(x)} \quad \dfrac{\dfrac{\mathrm{Odd}(y) \vdash \mathrm{Nat}(y)}{\mathrm{Odd}(y) \vdash \mathrm{Nat}(\mathrm{succ}\ y)}}{x = \mathrm{succ}\ y, \mathrm{Odd}(y) \vdash \mathrm{Nat}(x)}}{\mathrm{Even}(x) \vdash \mathrm{Nat}(x)}\,(\mathrm{Case}_{\mathrm{Even}}) \quad \dfrac{\dfrac{\dfrac{\mathrm{Even}(y) \vdash \mathrm{Nat}(y)}{\mathrm{Even}(y) \vdash \mathrm{Nat}(\mathrm{succ}\ y)}}{x = \mathrm{succ}\ y, \mathrm{Even}(y) \vdash \mathrm{Nat}(x)}}{\mathrm{Odd}(x) \vdash \mathrm{Nat}(x)}\,(\mathrm{Case}_{\mathrm{Odd}})}{\mathrm{Even}(x) \vee \mathrm{Odd}(x) \vdash \mathrm{Nat}(x)}$$

Explicit induction rules

For an inductive definition set, we can (systematically) derive a corresponding explicit induction rule:

$$\frac{\Gamma \vdash \boxed{F}(0) \qquad \Gamma, \boxed{F}(x) \vdash \boxed{F}(\mathrm{succ}\ x) \qquad \Gamma, \boxed{F}(t) \vdash \phi}{\Gamma, \mathrm{Nat}(t) \vdash \phi}\ (\mathrm{Ind}_{\mathrm{Nat}})$$

Notice how we have to choose a **inductive invariant** F.

A proof of the statement on the previous slide using explicit induction rules like this (and no cycles) requires a *choice* of F - this is less than ideal for proof search.

Case/(Un)folding rules

In cyclic systems, you replace explicit induction rules with case/(un)folding rules and cycles:

$$\frac{\Gamma, t = 0 \vdash \phi \qquad \Gamma, t = \mathrm{succ}\ x, \boxed{\mathrm{Nat}(x)} \vdash \phi}{\Gamma, \mathrm{Nat}(t) \vdash \phi} \ (\mathrm{Case}_{\mathrm{Nat}})$$

No **invariant** required!

Inductive predicate exists in the premise

$$\frac{\Gamma, t = 0 \vdash \phi \qquad \Gamma, t = \mathrm{succ}\ x, \boxed{\mathrm{Odd}(x)} \vdash \phi}{\Gamma, \mathrm{Even}(t) \vdash \phi} \ (\mathrm{Case}_{\mathrm{Even}})$$

Why do we require a trace condition?

$$\boxed{\frac{\mathrm{Bad}}{\mathrm{Bad}}}$$

This trace doesn't **progress**!

$$\dfrac{\dfrac{\vdash \mathrm{Bad}}{\vdash \mathrm{Bad}}\,(\mathrm{Bad}_R) \qquad \dfrac{\mathrm{Bad} \vdash \bot}{\mathrm{Bad} \vdash \bot}\,(\mathrm{Case}_{\mathrm{Bad}})}{\vdash \bot}\,(\mathrm{cut})$$

Cyclic **pre**-proof ✔

> Proof is **locally** well-formed

Cyclic proof ✘

> **Global** trace condition is not satisfied for the left cycle

Inductive predicates → fixed-point operators

Systems with (least) fixed-point operators also allow for the definition of inductive predicates:

$$\frac{}{\mathrm{Nat}(0)} \qquad \frac{\mathrm{Nat}(x)}{\mathrm{Nat}(\mathrm{succ}\ x)}$$

$$\mathrm{Nat} := \underbrace{\mu X.\lambda x.\boxed{x = 0} \vee \boxed{\exists y.x = \mathrm{succ}\ y \wedge X(y)}}_{\text{Must be \textbf{positive} in } X\text{!}}$$

$\_ \geq y := \mu(X : N \to \Omega).\lambda(x : N).x = y \vee \exists(z : N).x = \mathrm{succ}\ z \wedge X(z)$

The language of μHOL^{ex}

Type system with variances[3]

Fixed-point operators and ordinal approximations[2]

$$\boxed{v ::= + \mid - \mid 0}$$

$$\boxed{o ::= \alpha \mid \infty}$$

$$t ::= \boxed{x \mid \forall(x : T).t \mid t \Rightarrow t' \mid \lambda(x^{\boxed{v}} : T).t \mid t\ t'} \mid \boxed{\mu^{o}(x : P).t \mid \exists\alpha.t \mid \beta < \alpha}$$

Higher-order logic[1]

[1] [*Barendregt & Geuvers, 2001*] [2] [*Sprenger & Dam, 2003*] [3] [*Viswanathan & Viswanathan, 2004*]

Deduction system

Our deduction system extends the natural deduction style system of HOL with rules for fixed-points and fixed-point approximations:

Rules for fixed-points

$$\frac{\Gamma \vdash \phi[\mu^\infty(X : P).\phi / X]\ \vec{\psi}}{\Gamma \vdash (\mu^\infty(X : P).\phi)\ \vec{\psi}}\ (\text{fold}^\infty)$$

$$\frac{\Gamma \vdash (\mu^\infty(X : P).\phi)\ \vec{\psi}}{\Gamma \vdash \phi[\mu^\infty(X : P).\phi / X]\ \vec{\psi}}\ (\text{unfold}^\infty)$$

Rules for fixed-point approximations

$$\frac{\Gamma \vdash \exists \beta. \beta < \alpha \wedge \phi[\mu^\beta(X : P).\phi / X]\ \vec{\psi}}{\Gamma \vdash (\mu^\alpha(X : P).\phi)\ \vec{\psi}}\ (\text{fold}^\alpha)$$

$$\frac{\Gamma \vdash (\mu^\alpha(X : P).\phi)\ \vec{\psi}}{\Gamma \vdash \exists \beta. \beta < \alpha \wedge \phi[\mu^\beta(X : P).\phi / X]\ \vec{\psi}}\ (\text{unfold}^\alpha)$$

Deduction system

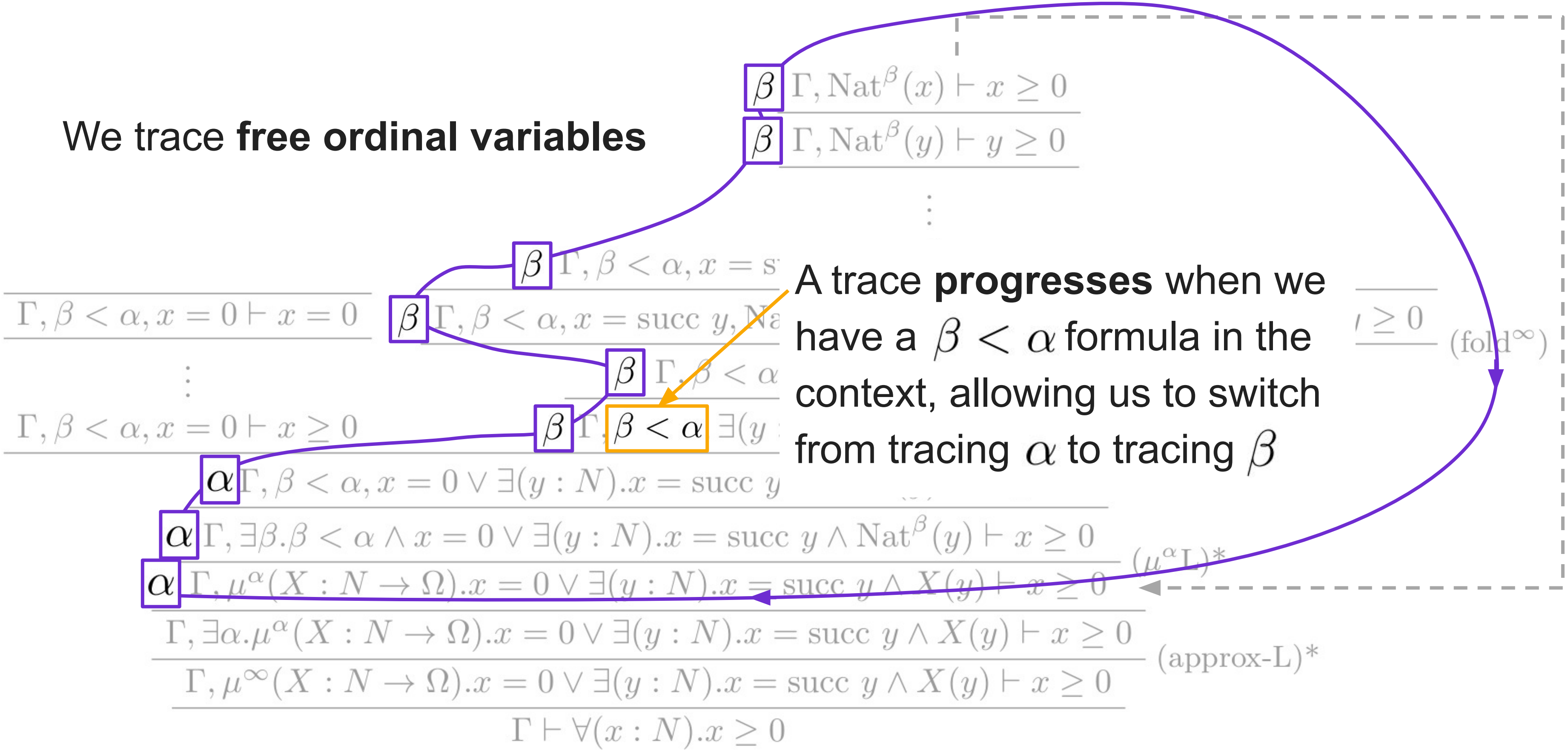
We have rules to **convert between** least fixed-points and their approximations:

$$\frac{\Gamma \vdash \exists \alpha.(\mu^{\alpha}(X : P).\phi)\ \vec{\psi}}{\Gamma \vdash (\mu^{\infty}(X : P).\phi)\ \vec{\psi}}\ \text{(promote)}$$

$$\frac{\Gamma \vdash (\mu^{\infty}(X : P).\phi)\ \vec{\psi}}{\Gamma \vdash \exists \alpha.(\mu^{\alpha}(X : P).\phi)\ \vec{\psi}}\ \text{(approx)}$$

Our trace condition

We trace **free ordinal variables**



Proof reduction → computational interpretation

In natural deduction style systems, there is often a good notion of proof reduction:

HOL

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma', \phi \vdash \phi}}{\vdots}}{\dfrac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi}} \qquad \dfrac{}{\Gamma \vdash \phi}}{\Gamma \vdash \psi} \qquad \longrightarrow \qquad \dfrac{\dfrac{}{\Gamma' \vdash \phi}}{\vdots \atop \Gamma \vdash \psi}$$

Move the direct proof of ϕ here

Proofs-as-programs interpretation

λHOL[1]

$$(\lambda(x : \phi).t)\ s \quad \longrightarrow_\beta \quad t[s/x]$$

[1] [*Barendregt & Geuvers, 2001*]

Proof reduction → computational interpretation

Our proofs can contain cycles, so we need to extend the notion of reduction (and our proofs-as-programs interpretation). For example, we want the following:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, (\mu^{\alpha} X.\phi)\ \vec{\psi} \vdash \chi}{\Gamma, \exists\alpha.(\mu^{\alpha} X.\phi)\ \vec{\psi} \vdash \chi}}{\Gamma, (\mu^{\infty} X.\phi)\ \vec{\psi} \vdash \chi}}{\Gamma \vdash (\mu^{\infty} X.\phi)\ \vec{\psi} \Rightarrow \chi} \qquad \dfrac{}{\Gamma \vdash (\mu^{\infty} X.\phi)\ \vec{\psi}}}{\Gamma \vdash \chi} \quad \longrightarrow^{*} \quad \begin{array}{c} \vdots \\ \Gamma \vdash \chi \end{array}$$

Some finite proof tree, where the cycle has been "unravelled"

Proof reduction → computational interpretation

$$
\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, \exists\alpha.\mathrm{Nat}^{\alpha}(3) \vdash 3 \geq 0}}{\Gamma, \mathrm{Nat}^{\infty}(3) \vdash 3 \geq 0}\;\text{(approx-L)*}}{\Gamma \vdash \mathrm{Nat}^{\infty}(3) \Rightarrow 3 \geq 0} \qquad \dfrac{}{\Gamma \vdash \mathrm{Nat}^{\infty}(3)}}{\Gamma \vdash 3 \geq 0}
\quad \longrightarrow^{*} \quad
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdots}}{\Gamma \vdash 0 \geq 0}}{\vdots}}{\Gamma \vdash 1 \geq 0}}{\dfrac{\dfrac{\vdots}{\Gamma \vdash 2 \geq 0}}{\dfrac{\vdots}{\Gamma \vdash 3 \geq 0}}}
$$

Proof reduction → computational interpretation

Represent cycles with recursion operators[1]

$$\mathrm{fix}^{\alpha} X^{\alpha}.t$$

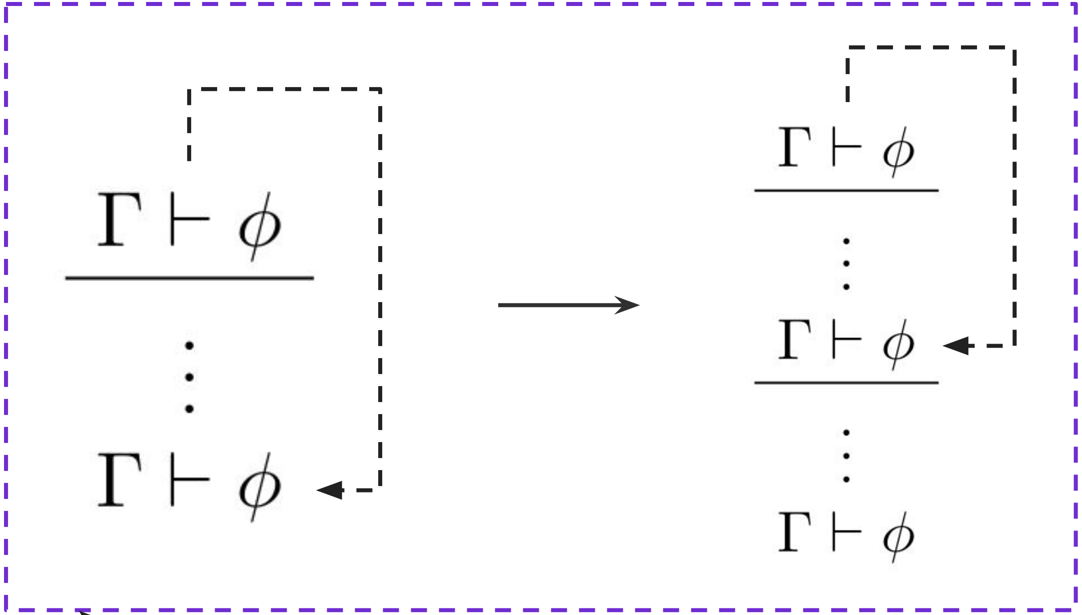
A form of pattern matching for elimination of ordinal approximation types

$$\mathrm{let}\ \langle \alpha, x \rangle := s\ \mathrm{in}\ t$$

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma, \exists\alpha.\mathrm{Nat}^{\alpha}(3) \vdash 3 \geq 0\end{array}}{\Gamma, \mathrm{Nat}^{\infty}(3) \vdash 3 \geq 0}\ (\text{approx-L})^*}{\Gamma \vdash \mathrm{Nat}^{\infty}(3) \Rightarrow 3 \geq 0} \qquad \dfrac{}{\Gamma \vdash \mathrm{Nat}^{\infty}(3)}}{\Gamma \vdash 3 \geq 0}$$

[1] [*Barlucchi, 2022*] [2] [*Barthe et al., 2004*]

Proof reduction → computational interpretation



The trace condition becomes a **type-based termination** argument under the proofs-as-programs interpretation.

$$\ldots X^{\beta} \ldots$$

PaP

$$\mathrm{fix}^{\alpha} X^{\alpha}.t \quad \to_{\mu} \quad \boxed{t}[\mathrm{fix}^{-} X^{-}.t/X^{-}]$$

Proof reduction → computational interpretation

$$
\begin{array}{l}
(\lambda(x : (\mu^{\infty} X.\phi)\ \vec{\psi}).\\
\quad \text{let } \langle \alpha, y \rangle := \text{approx}(x) \text{ in}\\
\quad \text{fix}^{\alpha}\ X^{\alpha}.t\\
)\ (\text{promote}\ \langle \iota, s \rangle)
\end{array}
\quad \xleftrightarrow{\textbf{PaP}} \quad
\dfrac{\dfrac{\dfrac{\dfrac{\Gamma, (\mu^{\alpha} X.\phi)\ \vec{\psi} \vdash \chi}{\Gamma, \exists \alpha.(\mu^{\alpha} X.\phi)\ \vec{\psi} \vdash \chi}}{\Gamma, (\mu^{\infty} X.\phi)\ \vec{\psi} \vdash \chi}}{\Gamma \vdash (\mu^{\infty} X.\phi)\ \vec{\psi} \Rightarrow \chi} \qquad \dfrac{}{\Gamma \vdash (\mu^{\infty} X.\phi)\ \vec{\psi}}}{\Gamma \vdash \chi}
$$

$$\downarrow_{\beta}$$

$$\text{let } \langle \alpha, y \rangle := \text{approx}(\text{promote}\ \langle \iota, s \rangle) \text{ in fix}^{\alpha}\ X^{\alpha}.t[\text{promote}\ \langle \iota, s \rangle / x]$$

$$\downarrow^{*}_{\beta\iota\mu}$$

$$t[\text{promote}\ \langle \iota, s \rangle / x][(\text{fix}^{-}\ X^{-}.t)/X^{-}][\iota/\alpha][s/y]$$

Proof reduction → computational interpretation

$$(\lambda(x : (\mu^\infty X.\phi)\ \vec{\psi}).$$
$$\quad \text{let } \langle \alpha, y\rangle := \text{approx}(x) \text{ in}$$
$$\quad \text{fix}^\alpha\ X^\alpha.t$$
$$)\ (\text{fold } s)$$

PaP

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\Gamma, (\mu^\alpha X.\phi)\ \vec{\psi} \vdash \chi}}{\Gamma, \exists\alpha.(\mu^\alpha X.\phi)\ \vec{\psi} \vdash \chi}}{\Gamma, (\mu^\infty X.\phi)\ \vec{\psi} \vdash \chi}}{\Gamma \vdash (\mu^\infty X.\phi)\ \vec{\psi} \Rightarrow \chi} \qquad \dfrac{\dfrac{}{\Gamma \vdash \phi[\mu^\infty X.\phi/X]\ \vec{\psi}}}{\Gamma \vdash (\mu^\infty X.\phi)\ \vec{\psi}}\ (\text{fold}^\infty)$$
$$\overline{\qquad\qquad\qquad\Gamma \vdash \chi\qquad\qquad\qquad}$$

$\to_\beta$

$$\text{let } \langle \alpha, y\rangle := \text{approx}(\text{fold } s) \text{ in fix}^\alpha\ X^\alpha.t[\text{fold } s/x]$$

stuck?

Proof reduction → computational interpretation

$$
\dfrac{\dfrac{\dfrac{\quad^{*}}{\Gamma \vdash \exists\alpha.\exists\beta.\beta < \alpha \wedge \phi[\mu^{\beta} X.\phi / X]\ \vec{\psi}}}{\Gamma \vdash \exists\alpha.(\mu^{\alpha} X.\phi)\ \vec{\psi}}}{\Gamma \vdash (\mu^{\infty} X.\phi)\ \vec{\psi}}\ (\text{promote})
$$

$$
\dfrac{\dfrac{}{\Gamma \vdash \phi[\mu^{\infty} X.\phi / X]\ \vec{\psi}}}{\Gamma \vdash (\mu^{\infty} X.\phi)\ \vec{\psi}}\ (\text{fold}^{\infty})
$$

An extra axiom…?

$$
\dfrac{}{\Gamma \vdash \exists\alpha.\beta < \alpha}\ (\text{next})
$$

Recap

We've discussed:

- Some background on cyclic proof theory
- Related systems and work we've built on
- The language and deduction system of $\mu\mathrm{HOL}^{ex}$
- Our trace condition using ordinal approximations
- Sketches of a computational interpretation for $\mu\mathrm{HOL}^{ex}$

Further work:

- Complete the computational interpretation of $\mu\mathrm{HOL}^{ex}$
- Study the system *without* explicit approximations (μHOL)
- Study the addition of fixed-point types and recursion operators (fix) to general PTS
- Study other links to existing systems (λ^, CoLF, Agda with sized types)

Thank you for listening! :)

Expressivity of higher-order logic

In a first-order system, terms like this would not be* definiable:

$$f : (N^0 \to \Omega)^+ \to \Omega \vdash \mu^\infty(X : N^0 \to \Omega).\lambda(x^0 : N).f\ X : N^0 \to \Omega$$

Notice that f is a predicate over *predicates over* N.

Depending on f, this fixed-point is either the total or empty predicate on N - this is provable within our system.