Implementing Observational Equality using Normalisation by Evaluation

Matthew Sirman **Meven Lennon-Bertrand** Neel Krishnaswami

UNIVERSITY OF CAMBRIDGE
Department of Computer Science and Technology

Types – June 12th 2024

A wunderkind meets another

For those who missed the hype I: observational equality

$$\text{Irrelevant}\ \frac{\Gamma \vdash p : t =_A u \qquad \Gamma \vdash q : t =_A u}{\Gamma \vdash p \cong q : t =_A u}$$

$$\text{Cast}\ \frac{\Gamma \vdash e : A =_{\mathcal{U}} A' \qquad \Gamma \vdash t : A}{\Gamma \vdash \mathbf{cast}(A, A', e, t) : A'}$$

For those who missed the hype I: observational equality

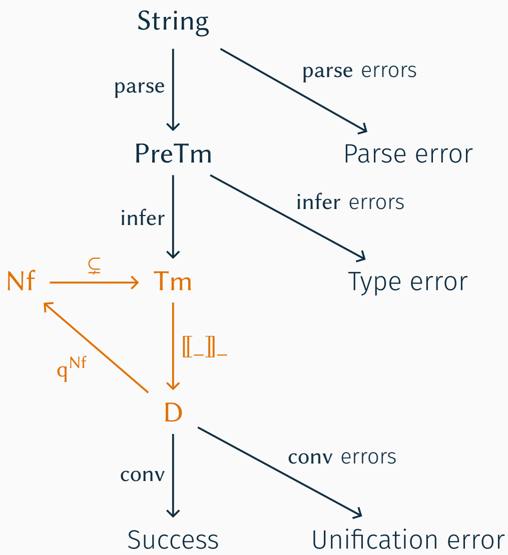
$$\text{Irrelevant}\ \frac{\Gamma \vdash p : t =_A u \qquad \Gamma \vdash q : t =_A u}{\Gamma \vdash p \cong q : t =_A u}$$

$$\text{Cast}\ \frac{\Gamma \vdash e : A =_{\mathcal{U}} A' \qquad \Gamma \vdash t : A}{\Gamma \vdash \mathbf{cast}(A, A', e, t) : A'}$$

$$\text{Cast}\Pi\ \frac{\Gamma \vdash e : \Pi\, x \colon A.B =_{\mathcal{U}} \Pi\, x \colon A'.B' \qquad \Gamma \vdash f : \Pi\, x \colon A.B \qquad \Gamma \vdash u : A'}{\Gamma \vdash \mathbf{cast}(\Pi\, x \colon A.B, \Pi\, x \colon A'.B', e, f)\ u \cong \mathbf{cast}(B[\ldots], B[u], \ldots, (f\ \mathbf{cast}(A', A, \ldots, u))) : B[u]}$$

$$\text{CastId}\ \frac{\Gamma \vdash e : A =_{\mathcal{U}} A' \qquad \Gamma \vdash A \cong A' \qquad \Gamma \vdash t : A}{\Gamma \vdash \mathbf{cast}(A, A', e, t) \cong t : A'}$$

For those who missed the hype II: NbE



The talk in one sentence

Normalisation by evaluation: it works![1]

[1] But you have to be a bit careful

Normalisation by evaluation: it works![1]

A collection of learned lessons.

[1] But you have to be a bit careful

NbE and definitional irrelevance

Ω: universe of **definitionally irrelevant** propositions

Interpreting proofs

Ω: universe of definitionally irrelevant propositions

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash p : \bot}{\Gamma \vdash \mathbf{abort}_A\ p : A}$$

Ω: universe of definitionally irrelevant propositions

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash p : \bot}{\Gamma \vdash \mathbf{abort}_A\ p : A}$$

$$[\![\_]\!]\_ \quad : \quad \mathsf{Tm} \to \mathsf{Env} \to \mathsf{D}$$

$$[\![\mathbf{abort}_A\ p]\!]\rho \quad = \quad ??$$

Interpreting proofs

Ω: universe of definitionally irrelevant propositions

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash p : \bot}{\Gamma \vdash \mathbf{abort}_A\ p : A}$$

$$[\![\_]\!]_\_ \quad : \quad \mathsf{Tm} \to \mathsf{Env} \to \mathsf{D}$$

$$[\![\mathbf{abort}_A\ p]\!]\rho \quad = \quad \uparrow(\mathsf{Abort}\ [\![A]\!]\rho\ [\![p]\!]\rho)$$

Interpreting proofs

Ω: universe of **definitionally irrelevant** propositions

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash p : \bot}{\Gamma \vdash \mathbf{abort}_A\ p : A}$$

$$\begin{aligned}
[\![_]\!]^{\mathcal{U}}_{_} \quad &: \quad \mathsf{Tm} \rightarrow \mathsf{Env} \rightarrow \mathsf{D}^{\mathcal{U}} \\
[\![\mathbf{abort}_A\ p]\!]^{\mathcal{U}} \rho \quad &= \quad \uparrow\!\left(\mathsf{Abort}\ \left([\![A]\!]^{\mathcal{U}} \rho\right)\ \left([\![p]\!]^{\Omega} \rho\right)\right) \\
\\
[\![_]\!]^{\Omega}_{_} \quad &: \quad \mathsf{Tm} \rightarrow \mathsf{Env} \rightarrow \mathsf{D}^{\Omega} \\
&\ldots
\end{aligned}$$

Ω: universe of definitionally irrelevant propositions

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash p : \bot}{\Gamma \vdash \mathbf{abort}_A\ p : A}$$

$$\begin{aligned}
[\![_]\!]^{\mathcal{U}}_{_} \quad &: \quad \mathsf{Tm} \to \mathsf{Env} \to \mathsf{D}^{\mathcal{U}} \\
[\![\mathbf{abort}_A\ p]\!]^{\mathcal{U}}\rho \quad &= \quad \uparrow(\mathsf{Abort}\ ([\![A]\!]^{\mathcal{U}}\rho)\ ([\![p]\!]^{\Omega}\rho)) \\
\\
[\![_]\!]^{\Omega}_{_} \quad &: \quad \mathsf{Tm} \to \mathsf{Env} \to \mathsf{D}^{\Omega} \\
&\dots
\end{aligned}$$

We must decide which evaluation to use **based on the term only**:

$$[\![t\ u]\!]^{\mathcal{U}}\rho \quad = \quad \underline{\mathsf{app}}\,([\![t]\!]^{\mathcal{U}}\rho)\ ([\![u]\!]^{?}\rho)$$

Ω: universe of definitionally irrelevant propositions

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash p : \bot}{\Gamma \vdash \mathbf{abort}_A\ p : A}$$

$$[\![\_]\!]^{\mathcal{U}}\_ \quad : \quad \mathsf{Tm} \to \mathsf{Env} \to \mathsf{D}^{\mathcal{U}}$$

$$[\![\mathbf{abort}_A\ p]\!]^{\mathcal{U}} \rho \quad = \quad \uparrow\!\left(\mathsf{Abort}\ \left([\![A]\!]^{\mathcal{U}} \rho\right)\ \left([\![p]\!]^{\Omega} \rho\right)\right)$$

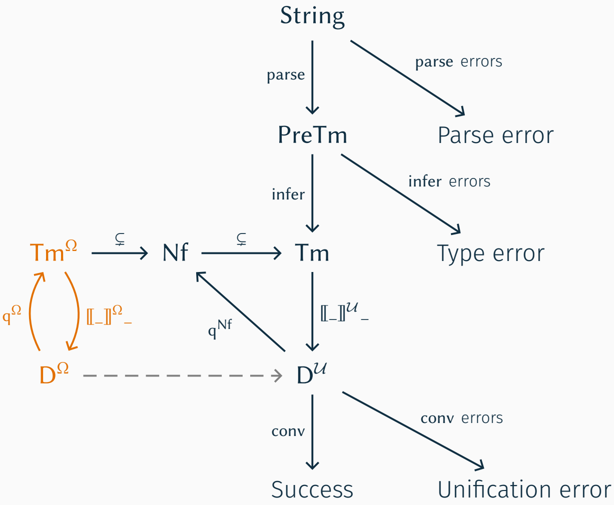
$$[\![\_]\!]^{\Omega}\_ \quad : \quad \mathsf{Tm} \to \mathsf{Env} \to \mathsf{D}^{\Omega}$$

$$\ldots$$

We must decide which evaluation to use **based on the term only**:

$$[\![t\ u^{\mathfrak{s}}]\!]^{\mathcal{U}} \rho \quad = \quad \underline{\mathsf{app}}\left([\![t]\!]^{\mathcal{U}} \rho\right)\ \left([\![u]\!]^{\mathfrak{s}} \rho\right)$$

What should D^Ω be?



Attempt 1: unit type

This is easy! "A Modular Type-Checking Algorithm for Type Theory with Singleton Types and Proof Irrelevance" (Abel et al., 2009):

$$\begin{aligned} \mathrm{D}^{\Omega} &:= 1 \\ [\![p]\!]^{\Omega}\rho &:= ! \end{aligned}$$

Attempt 1: unit type

This is easy! “A Modular Type-Checking Algorithm for Type Theory with Singleton Types and Proof Irrelevance” (Abel et al., 2009):

$$
\begin{aligned}
\mathrm{D}^{\Omega} &:= 1 \\
[\![p]\!]^{\Omega}\rho &:= \,!
\end{aligned}
$$

+ very simple
- quoting is lost
  - ? no more printing to the user
  - - no more meta-variable solving

Attempt 1: unit type

This is easy! “A Modular Type-Checking Algorithm for Type Theory with Singleton Types and Proof Irrelevance” (Abel et al., 2009):

$$\mathrm{D}^{\Omega} := 1$$

$$[\![p]\!]^{\Omega}\rho := !$$

+ very simple
- quoting is lost
  - ? no more printing to the user
  - \- no more meta-variable solving

Solution? Add an inhabitant to all propositions, lose consistency...

Attempt 2: terms

$$
\begin{aligned}
\mathrm{D}^{\Omega} &:= \mathsf{Env} \times \mathsf{Tm}^{\Omega} \\
[\![p]\!]^{\Omega}\rho &:= (\rho, p)
\end{aligned}
$$

Attempt 2: terms

$$\mathsf{D}^{\Omega} \quad := \quad \mathsf{Env} \times \mathsf{Tm}^{\Omega}$$

$$[\![p]\!]^{\Omega}\rho \quad := \quad (\rho, p)$$

+ quoting is possible: quote ρ, substitute in p
- difficult to manipulate propositions:

$$\mathbf{cast}(\Pi\, x\colon A.B, \Pi\, x\colon A'.B', e, f)\; u \cong \mathbf{cast}(B[u'], B[u], (\mathbf{snd}\; e)\; u, (f\; u'))$$

→ quoting and evaluation must be mutual

Attempt 3: a different domain

A domain

- similar to $\mathrm{D}^{\mathcal{U}}$: de Bruijn levels, closures
- represents *all* terms: $\mathrm{PApp}_{\mathfrak{S}} : \mathrm{D}^{\Omega} \to \mathrm{D}^{\Omega} \to \mathrm{D}^{\Omega}$ (vs $\mathrm{App}_{\mathfrak{S}} : \mathrm{D}^{\mathrm{ne}} \to \mathrm{D}^{\mathfrak{S}} \to \mathrm{D}^{\mathcal{U}}$)
- closures used only during quoting

A domain

- similar to $\mathrm{D}^{\mathcal{U}}$: de Bruijn levels, closures
- represents *all* terms: $\mathrm{PApp}_{\mathfrak{s}} : \mathrm{D}^{\Omega} \to \mathrm{D}^{\Omega} \to \mathrm{D}^{\Omega}$ (vs $\mathrm{App}_{\mathfrak{s}} : \mathrm{D}^{\mathrm{ne}} \to \mathrm{D}^{\mathfrak{s}} \to \mathrm{D}^{\mathcal{U}}$)
- closures used only during quoting

New! : Freezing a relevant value: $\phi : \mathrm{D}^{\mathcal{U}} \to \mathrm{D}^{\Omega}$

$$[\![x]\!]^{\Omega}\rho \quad := \quad \phi(\rho\ x) \quad \text{if the entry } x \text{ is relevant}$$

Conversion and unification

Conversion

$$\_ \vdash \_ \cong \_ \quad : \quad \text{Nat} \to \text{D}^{\mathcal{U}} \to \text{D}^{\mathcal{U}} \to \text{Option Error}$$

Conversion

$$\_ \vdash \_ \cong \_ \quad : \quad \mathsf{Nat} \to \mathsf{D}^{\mathcal{U}} \to \mathsf{D}^{\mathcal{U}} \to \mathsf{Option\ Error}$$

Ignores irrelevant subterms:

$$\frac{\Gamma \vdash\uparrow e \cong\uparrow e' \qquad \Gamma \vdash a \cong a'}{\Gamma \vdash \uparrow(\mathsf{App}_{\mathcal{U}}\ e\ a) \cong\uparrow(\mathsf{App}_{\mathcal{U}}\ e'\ a')} \qquad \frac{\Gamma \vdash \uparrow e \cong \uparrow e'}{\Gamma \vdash \uparrow(\mathsf{App}_{\Omega}\ e\ p) \cong \uparrow(\mathsf{App}_{\Omega}\ e'\ \ p')}$$

The landmark rule of "Impredicative Observational Equality" (Pujet et al., 2023):

$$\text{CastId}\ \frac{\Gamma \vdash e : A =_{\mathcal{U}} A' \qquad \Gamma \vdash A \cong A' \qquad \Gamma \vdash t : A}{\Gamma \vdash \mathbf{cast}(A, A', e, t) \cong t : A'}$$

The landmark rule of "Impredicative Observational Equality" (Pujet et al., 2023):

$$\text{CastId}\ \frac{\Gamma \vdash e : A =_{\mathcal{U}} A' \qquad \Gamma \vdash A \cong A' \qquad \Gamma \vdash t : A}{\Gamma \vdash \mathbf{cast}(A, A', e, t) \cong t : A'}$$

A reduction/evaluation rule?

- **+** conceptually simple
- **?** confluence?
- **-** makes conversion and reduction mutual

Identity casts in conversion

$$\textsc{CastEqL}\ \frac{\Gamma \vdash A \cong B \qquad \Gamma \vdash a \cong a'}{\Gamma \vdash \mathsf{Cast}\ A\ B\ e\ a \cong a'} \qquad \textsc{CastEqR}\ \frac{\Gamma \vdash A' \cong B' \qquad \Gamma \vdash a \cong a'}{\Gamma \vdash a \cong \mathsf{Cast}\ A'\ B'\ e'\ a'}$$

$$\textsc{CastEqCong}\ \frac{\Gamma \vdash A \cong A' \qquad \Gamma \vdash B \cong B' \qquad \Gamma \vdash a \cong a'}{\Gamma \vdash \mathsf{Cast}\ A\ B\ e\ a \cong \mathsf{Cast}\ A'\ B'\ e'\ a'}$$

1. eagerly apply CastEqL and CastEqR
2. if they fail, backtrack and use CastEqCong

Somewhat similar to term-directed η-expansion

Metavariables!

Contextual meta-variables $?m[\rho]$, and sort (meta-)variables.

Metavariables!

Contextual meta-variables $?m[\rho]$, and sort (meta-)variables.

$$\frac{\rho' = \mathsf{invert}(\rho) \qquad t = \mathsf{rename}^{\Delta}_{?m_i}\ a\ \rho'}{(\Sigma, ?m_i, \Sigma'); \Delta \vdash ?m_i[\rho] \cong t; (\Sigma, ?m_i := t, \Sigma')}$$

Imho, simpler and conceptually cleaner than λ-lifting

Wrapping up

```
let f : ℕ → ℕ =
  λx. S x
in
let x : ℕ =
  S (S (S 0))
in
f ?{f, x}
```

```
[error]: Found proof goal.
     ╭──▶ <test-file>@8:7-8:14
   8 │      f ?{f, x}
     •        ───────
     •        ╰╸ Expected type [ℕ] at goal.
     •
     •           List of relevant terms and their types:
     •           f : ℕ → ℕ
     •           x : ℕ
─────╯
```

Some extra remarks

- equality and casts as destructors on the universe → reflected semantically
- **refl** and friends are also destructors → annotated, *infer*
- defunctionalised NbE → *lots* of closures

Some extra remarks

- equality and casts as destructors on the universe → reflected semantically
- **refl** and friends are also destructors → annotated, *infer*
- defunctionalised NbE → *lots* of closures

Extensions I will not talk about:

- quotients → very straightforward
- first-class, indexed-ish inductive types → much less
  (anybody knows about Mendler-style + dependent types?)

Normalisation by evaluation: it works![1]

Thank you!

[1]But you have to be a bit careful