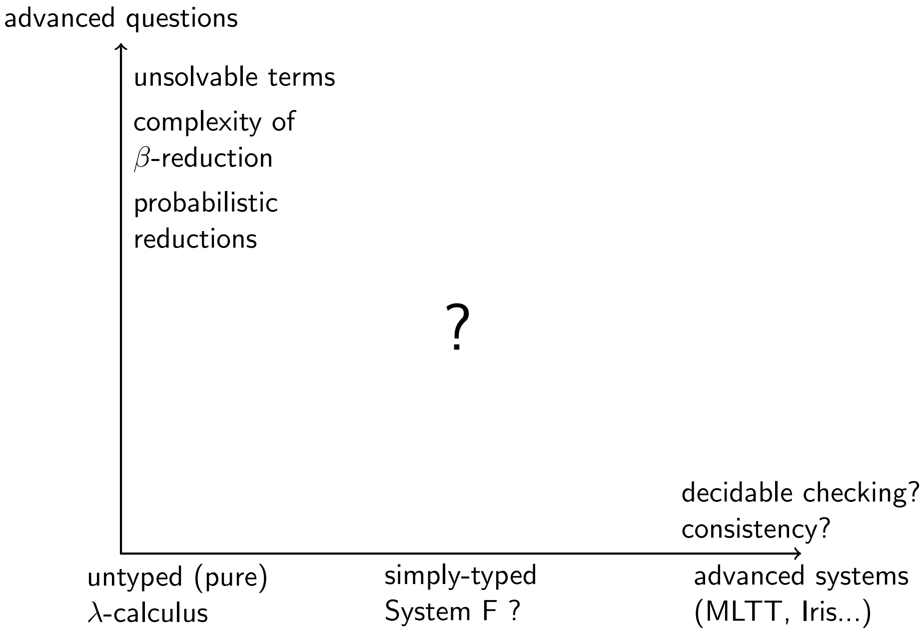
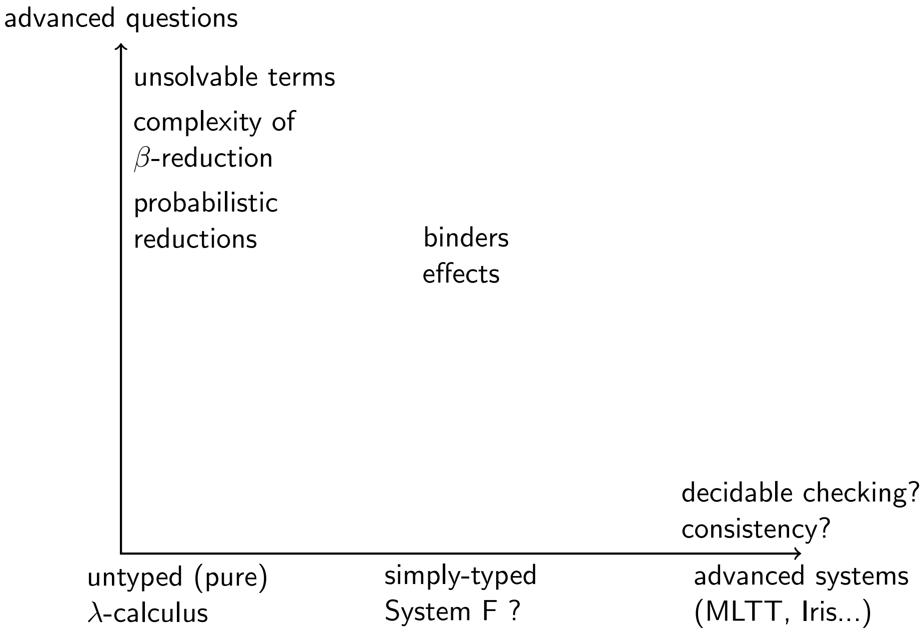
Proof theory for type systems

Gabriel Scherer

Parsifal, INRIA Saclay (Paris area)

January 22, 2018


advanced questions
unsolvable terms
complexity of β-reduction
probabilistic reductions
?
decidable checking?
consistency?
untyped (pure) λ-calculus
simply-typed
System F ?
advanced systems
(MLTT, Iris...)


advanced questions
unsolvable terms
complexity of β-reduction
probabilistic reductions
binders
effects
decidable checking?
consistency?
untyped (pure) λ-calculus
simply-typed
System F ?
advanced systems (MLTT, Iris...)

advanced questions

unsolvable terms

complexity of
β-reduction

probabilistic
reductions

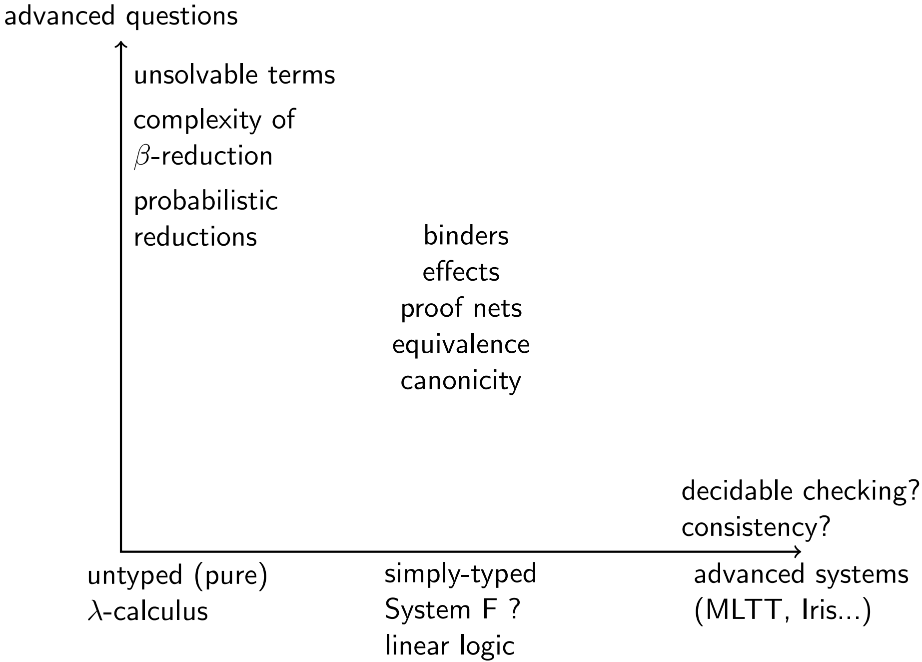
binders
effects
proof nets

decidable checking?
consistency?

untyped (pure)
λ-calculus

simply-typed
System F ?
linear logic

advanced systems
(MLTT, Iris...)


advanced questions
unsolvable terms
complexity of
β-reduction
probabilistic
reductions
binders
effects
proof nets
equivalence
canonicity
decidable checking?
consistency?
untyped (pure)
λ-calculus
simply-typed
System F ?
linear logic
advanced systems
(MLTT, Iris...)

Section 1

Focusing

Focusing

Focusing is a technique from proof theory [Andreoli, 1992].

It studies **invertibility** of connectives
to structure the search space.

Type theory perspective: canonical representations.

$$t \approx_{\beta\eta} u \qquad \overset{?}{\Longrightarrow} \qquad t \approx_{\alpha} u$$

$$\frac{\Gamma \vdash \underline{A} \qquad \Gamma, \underline{B} \vdash C}{\Gamma, \underline{A \to B} \vdash C}\ -$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}$$

$$\frac{\Gamma, \underline{A_i} \vdash C}{\Gamma, \underline{A_1 \times A_2} \vdash C}\ -$$

$$\frac{\Gamma \vdash A_1 \qquad \Gamma \vdash A_2}{\Gamma \vdash A_1 \times A_2}$$

$$\frac{\Gamma, A_1 \vdash C \qquad \Gamma, A_2 \vdash C}{\Gamma, A_1 + A_2 \vdash C}$$

$$\frac{\Gamma \vdash \underline{A_i}}{\Gamma \vdash \underline{A_1 + A_2}}\ +$$

$$\frac{}{\Gamma, 0 \vdash C}\ +$$

$$\frac{}{\Gamma \vdash 1}\ -$$

Invertible vs. non-invertible rules. Positives vs. negatives.

$$\frac{\Gamma \vdash \underline{A} \qquad \Gamma, \underline{B} \vdash C}{\Gamma, \underline{A \to B} \vdash C}\, - \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}$$

$$\frac{\Gamma, \underline{A_i} \vdash C}{\Gamma, \underline{A_1 \times A_2} \vdash C}\, - \qquad \frac{\Gamma \vdash A_1 \qquad \Gamma \vdash A_2}{\Gamma \vdash A_1 \times A_2}$$

$$\frac{\Gamma, A_1 \vdash C \qquad \Gamma, A_2 \vdash C}{\Gamma, A_1 + A_2 \vdash C} \qquad \frac{\Gamma \vdash \underline{A_i}}{\Gamma \vdash \underline{A_1 + A_2}}\, +$$

$$\frac{}{\Gamma, 0 \vdash C}\, + \qquad \frac{}{\Gamma \vdash 1}\, -$$

Invertible vs. non-invertible rules. Positives vs. negatives.

$$N, M ::= A \to B \mid A \times B \mid 1 \qquad P, Q ::= A + B \mid 0$$

$$A, B ::= P \mid N \mid \alpha \qquad P_a, Q_a ::= P \mid \alpha \qquad N_a, M_a ::= N \mid \alpha$$

Invertible phase

$$\dfrac{\dfrac{?}{\alpha + \beta \vdash \alpha}}{\alpha + \beta \vdash \beta + \alpha}$$

If applied too early, non-invertible rules can ruin your proof.

Focusing restriction 1: invertible phases

Invertible rules must be applied as soon and as long as possible
– and their order does not matter.

Invertible phase

$$\dfrac{\dfrac{?}{\alpha + \beta \vdash \alpha}}{\alpha + \beta \vdash \beta + \alpha}$$

If applied too early, non-invertible rules can ruin your proof.

Focusing restriction 1: invertible phases

Invertible rules must be applied as soon and as long as possible
– and their order does not matter.

Imposing this restriction gives a single proof of $(\alpha \to \beta) \to (\alpha \to \beta)$ instead of two ($\lambda f.\, f$ and $\lambda f.\, \lambda x.\, f\ x$).

After all invertible rules, negative context Γ_{na}, positive goal P_{a}.

Non-invertible phases

After all invertible rules, negative context, positive goal.

Only step forward: select a formula, apply some non-invertible rule on it.

Non-invertible phases

After all invertible rules, negative context, positive goal.

Only step forward: select a formula, apply some non-invertible rule on it.

Focusing restriction 2: non-invertible phase

When a principal formula is selected for non-invertible rule, they should be applied as long as possible – until its polarity changes.

Non-invertible phases

After all invertible rules, negative context, positive goal.

Only step forward: select a formula, apply some non-invertible rule on it.

Focusing restriction 2: non-invertible phase

When a principal formula is selected for non-invertible rule, they should be applied as long as possible – until its polarity changes.

Completeness: this restriction preserves provability. **Non-trivial !**
Example of removed redundancy:

$$\dfrac{\dfrac{\dfrac{\alpha_2, \quad \beta_1 \vdash A}{\alpha_2 \times \alpha_3, \quad \beta_1 \vdash A}}{\alpha_2 \times \alpha_3, \quad \beta_1 \times \beta_2 \vdash A}}{\alpha_1 \times \alpha_2 \times \alpha_3, \beta_1 \times \beta_2 \vdash A}$$

This was focusing:

- invertible as long as a rule matches, until $\Gamma_{\mathsf{na}} \vdash P_{\mathsf{a}}$
- then pick a formula
- then non-invertible as long as a rule matches, until polarity change

Completeness:

$$\Gamma \vdash A \qquad \Longrightarrow \qquad \Gamma \vdash_{\texttt{foc}} A$$

a focused natural deduction

$$N, M ::= A \to B \mid A \times B \mid 1 \qquad P, Q ::= A + B \mid 0$$

$$A, B ::= P \mid N \mid \alpha \qquad P_\mathsf{a}, Q_\mathsf{a} ::= P \mid \alpha \qquad N_\mathsf{a}, M_\mathsf{a} ::= N \mid \alpha$$

$$\Gamma_\mathsf{na} ::= \emptyset \mid \Gamma_\mathsf{na}, N_\mathsf{a}$$

$\Gamma_\mathsf{na}; \Delta \vdash_\mathsf{inv} A$ invertible phase (decomposes Δ, A)

$\Gamma_\mathsf{na} \vdash_\mathsf{foc} P_\mathsf{a}$ choice of focus

$\Gamma_\mathsf{na}; N \Downarrow M_\mathsf{a}$ non-invertible negative rules

$\Gamma_\mathsf{na} \Uparrow P$ non-invertible positive rules

(inspired by Brock-Nannestad and Schürmann [2010])

$$\frac{\Gamma_{na}; \Delta, P \vdash_{inv} N}{\Gamma_{na}; \Delta \vdash_{inv} P \to N} \qquad \frac{(\Gamma_{na}; \Delta \vdash_{inv} N_i)^i}{\Gamma_{na}; \Delta \vdash_{inv} N_1 \times N_2} \qquad \frac{(\Gamma_{na}; \Delta, Q_i \vdash_{inv} A)^i}{\Gamma_{na}; \Delta, Q_1 + Q_2 \vdash_{inv} A}$$

$$\frac{}{\Gamma_{na}; \Delta, 0 \vdash_{inv} A} \qquad \frac{}{\Gamma_{na}; \Delta \vdash_{inv} 1} \qquad \frac{\Gamma_{na}, \Gamma'_{na} \vdash_{foc} P_a}{\Gamma_{na}; \Gamma'_{na} \vdash_{inv} P_a}$$

$$\frac{\Gamma_{na} \Uparrow P}{\Gamma_{na} \vdash_{foc} P} \qquad \frac{\Gamma_{na}, N; N \Downarrow \alpha}{\Gamma_{na}, N \vdash_{foc} \alpha} \qquad \frac{\Gamma_{na}, N; N \Downarrow P \qquad \Gamma_{na}; P \vdash_{inv} Q_a}{\Gamma_{na}, N \vdash_{foc} Q_a}$$

$$\frac{\Gamma_{na} \Uparrow P_i}{\Gamma_{na} \Uparrow P_1 + P_2} \qquad \frac{}{\Gamma_{na}, \alpha \Uparrow \alpha} \qquad \frac{\Gamma_{na}; \emptyset \vdash_{inv} N}{\Gamma_{na} \Uparrow N}$$

$$\frac{}{\Gamma_{na}; N \Downarrow N} \qquad \frac{\Gamma_{na}; N \Downarrow M_{a1} \times M_{a2}}{\Gamma_{na}; N \Downarrow M_{ai}} \qquad \frac{\Gamma_{na}; N \Downarrow P \to M \qquad \Gamma_{na} \Uparrow P}{\Gamma_{na}; N \Downarrow M}$$

(some simplifications, see Scherer [2016] for full details)

Section 2

Focused λ-calculus

β-normal forms (negative)

β-short normal forms:

$$\pi_1\ (t, u) = t$$

$$\begin{array}{rcl} v, w & ::= & \lambda x.\, v \mid (v, w) \mid n \\ n, m & ::= & \pi_i\ n \mid n\ v \mid x \end{array}$$

β-normal forms (negative)

β-short normal forms:

$$\pi_1\ (t, u) = t$$

$$\begin{array}{lcl} v, w & ::= & \lambda x.\, v \mid (v, w) \mid n \\ n, m & ::= & \pi_i\ n \mid n\ v \mid x \end{array}$$

β-short η-long:

$$(y : \alpha \to \beta) = \lambda x : \alpha.\, (y\ x : \beta)$$

β-normal forms (negative)

β-short normal forms:

$$\pi_1\,(t, u) = t$$

$$\begin{array}{rcl} v, w & ::= & \lambda x.\, v \mid (v, w) \mid n \\ n, m & ::= & \pi_i\ n \mid n\ v \mid x \end{array}$$

β-short η-long:

$$(y : \alpha \to \beta) = \lambda x : \alpha.\, (y\ x : \beta)$$

$$\begin{array}{rcl} v, w & ::= & \lambda x.\, v \mid (v, w) \mid (n : \alpha) \\ n, m & ::= & \pi_i\ n \mid n\ v \mid x \end{array}$$

What about sums?

$$
\begin{array}{rcl}
v, w & ::= & \lambda x.\, v \mid (v, w) \mid \sigma_i\ v \mid (n : \alpha) \\
n, m & ::= & \pi_i\ n \mid n\ v \mid \left(\texttt{match}\ n\ \texttt{with} \left| \begin{array}{l} \sigma_1\ y_1 \to v_1 \\ \sigma_2\ y_2 \to v_2 \end{array} \right. \right) \mid x
\end{array}
$$

Does not work:

$$
\left(\begin{array}{l} \texttt{match}\ n\ \texttt{with} \\ \left| \begin{array}{l} \sigma_1\ y_1 \to \lambda z.\, v_1 \\ \sigma_2\ y_2 \to \lambda z.\, v_2 \end{array} \right. \end{array} \right) v
\qquad\qquad
\begin{array}{l} \texttt{match}\ n\ \texttt{with} \\ \left| \begin{array}{l} \sigma_1\ x \to \sigma_2\ x \\ \sigma_2\ x \to \sigma_1\ x \end{array} \right. \end{array}
$$

Focusing to the rescue

$$
\begin{aligned}
v, w &::= \lambda x.\, v \mid (v, w) \mid (n : \alpha) \\
n, m &::= \pi_i\ n \mid n\ v \mid x
\end{aligned}
$$

$$\Downarrow$$

$$
\begin{aligned}
v, w ::= {} & \lambda x.\, v \mid (v, w) \mid () \\
& \mid \mathtt{absurd}(x) \mid \left(\mathtt{match}\ x\ \mathtt{with} \left| \begin{array}{l} \sigma_1\ y_1 \to v_1 \\ \sigma_2\ y_2 \to v_2 \end{array} \right. \right) \\
& \mid (\Gamma_{\mathsf{na}} \vdash f : P_{\mathsf{a}})
\end{aligned}
$$

$$
\begin{aligned}
n, m &::= \pi_i\ n \mid n\ p \mid x \\
p, q &::= \sigma_i\ p \mid (v : N_{\mathsf{a}})
\end{aligned}
$$

$$
f \quad ::= (n : \alpha) \mid (p : P) \mid \mathtt{let}\ x = (n : P)\ \mathtt{in}\ v
$$

(See also Munch-Maccagnoni [2013])

Completeness of focusing

Logic:

$$\Gamma \vdash A \qquad \Longrightarrow \qquad \Gamma \vdash_{\texttt{foc}} A$$

Completeness of focusing

Logic:

$$\Gamma \vdash A \qquad \Longrightarrow \qquad \Gamma \vdash_{\mathtt{foc}} A$$

Programming:

$$\Gamma \vdash t : A \qquad \Longrightarrow \qquad \exists v, \begin{array}{c} \Gamma \vdash_{\mathtt{foc}} v : A \\ v \approx_{\beta\eta} t \end{array}$$

Canonicity

Focused normal forms are canonical for the impure λ-calculus.

Proof in Zeilberger [2009], using ideas from Girard's ludics.

Canonicity

Focused normal forms are canonical for the impure λ-calculus.

Proof in Zeilberger [2009], using ideas from Girard's ludics.

Not canonical for the **pure** calculus.

$$\texttt{let}\ x = n\ \texttt{in}\ C\left[\texttt{let}\ x' = n'\ \texttt{in}\ v\right]$$

$$\texttt{let}\ x' = n'\ \texttt{in}\ C\left[\texttt{let}\ x = n\ \texttt{in}\ v\right]$$

Canonicity

Focused normal forms are canonical for the impure λ-calculus.

Proof in Zeilberger [2009], using ideas from Girard's ludics.

Not canonical for the **pure** calculus.

$$\texttt{let}\ x = n\ \texttt{in}\ C\left[\texttt{let}\ x' = n'\ \texttt{in}\ v\right]$$

$$\texttt{let}\ x' = n'\ \texttt{in}\ C\left[\texttt{let}\ x = n\ \texttt{in}\ v\right]$$

Solution: "saturation" [Scherer, 2017]

$$f \quad ::= \quad \texttt{let}\ \bar{x} = \bar{n}\ \texttt{in}\ v \mid (n : \alpha) \mid (p : P)$$

inspired by multi-focusing [Chaudhuri, Miller, and Saurin, 2008].

Recap

$$
\begin{array}{lll}
\Gamma_{\mathsf{na}}; \Delta \vdash_{\mathsf{inv}} v : A & v, w ::= & \lambda x.\, v \mid (v, w) \mid () \\
& & \mid \mathtt{absurd}(x) \mid \mathtt{match}\ x\ \mathtt{with} \left| \begin{array}{l} \sigma_1\ y_1 \to v_1 \\ \sigma_2\ y_2 \to v_2 \end{array} \right. \\
& & \mid (\Gamma_{\mathsf{na}} \vdash f : P_{\mathsf{a}}) \\
\\
\Gamma_{\mathsf{na}} \vdash n \Downarrow N_{\mathsf{a}} & n, m ::= & \pi_i\ n \mid n\ p \mid x \\
\Gamma_{\mathsf{na}} \vdash p \Uparrow P_{\mathsf{a}} & p, q ::= & \sigma_i\ p \mid (v : N_{\mathsf{a}}) \\
\\
\Gamma_{\mathsf{na}} \vdash_{\mathsf{foc}} f : A & f ::= & \mathtt{let}\ \bar{x} = (n \mathrel{\bar{:}} P)\ \mathtt{in}\ v \\
& & \mid (n : \alpha) \mid (p : P)
\end{array}
$$

(plus saturation conditions)

(decision diagrams!
Altenkirch and Uustalu [2004], Ahmad, Licata, and Harper [2010])

Applications

A clean way to extend our understanding to positives $(+, 0)$.

- evaluation order in presence of effects
- which types have a unique inhabitant?
- decidability of equivalence
- Böhm separation results: contextual and $(\beta\eta)$ coincide
- λ-definability?
- (your result here!)

Section 3

Questions

Saturation for System F?

Termination of saturation: **subformula property**. Not in F!

$$\frac{\Gamma, A[B/\alpha] \vdash C}{\Gamma \ni \forall\alpha.\, A \vdash C}$$

Equivalence is undecidable in F: no decidable canonical forms.

Could we have a partial algorithm that works sometimes?

Eliminating polymorphism

Idea: probe the structure of $\forall\alpha.\, A$ through proof search.

$$\dfrac{\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \stackrel{\text{def}}{=} A \to B \to \alpha \vdash \alpha}}{\vdash \forall\alpha.\,(A \to B \to \alpha) \to \alpha}$$

Eliminating polymorphism

Idea: probe the structure of $\forall\alpha.\, A$ through proof search.

$$\dfrac{\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \stackrel{\text{def}}{=} A \to B \to \alpha \vdash \alpha}}{\vdash \forall\alpha.\,(A \to B \to \alpha) \to \alpha}
\qquad
\dfrac{\dfrac{\Gamma \vdash A \quad \oplus \quad \Gamma \vdash B}{\Gamma \stackrel{\text{def}}{=} A \to \alpha, B \to \alpha \vdash \alpha}}{\vdash \forall\alpha.\,(A \to \alpha) \to (B \to \alpha) \to \alpha}$$

Eliminating polymorphism

Idea: probe the structure of $\forall\alpha.\, A$ through proof search.

$$\dfrac{\dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \overset{\text{def}}{=} A \to B \to \alpha \vdash \alpha}}{\vdash \forall\alpha.\,(A \to B \to \alpha) \to \alpha}
\qquad
\dfrac{\dfrac{\Gamma \vdash A \quad \oplus \quad \Gamma \vdash B}{\Gamma \overset{\text{def}}{=} A \to \alpha, B \to \alpha \vdash \alpha}}{\vdash \forall\alpha.\,(A \to \alpha) \to (B \to \alpha) \to \alpha}$$

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \alpha} \quad \oplus \quad \dfrac{\dfrac{}{\Gamma \vdash \alpha \to \alpha} \qquad \Gamma \vdash \alpha}{\Gamma \vdash \alpha}}{\Gamma \overset{\text{def}}{=} \alpha \to \alpha, \alpha \vdash \alpha}}{\vdash \forall\alpha.\,(\alpha \to \alpha) \to \alpha \to \alpha}$$

(Ongoing discussions with Li-Yao Xia and Jean-Philippe Bernardy)

The place of bi-directional systems?

Bidirectional systems: natural fit for normal forms.

$$\frac{\Delta \in (x : T)}{\Delta \vdash x = x \in T} \qquad \frac{\Delta \vdash n_1 = n_2 \in (T \to U) \qquad \Delta \vdash T \ni v_1 = v_2}{\Delta \vdash n_1\ v_1 = n_2\ v_2 \in U}$$

$$\frac{\Delta, x : T \vdash U \ni v_1\ x = v_2\ x}{\Delta \vdash T \to U \ni v_1 = v_2} \qquad \frac{\Delta \vdash n_1 = n_2 \in \alpha}{\Delta \vdash \alpha \ni n_1 = n_2}$$

General programs? Program equivalence? Type inference?

Saturation in practice?

Is it possible to be efficient?

(in presence of software libraries?)

relations to program synthesis

Positives in richer systems?

η for sums:

$$C[\Box : A + B] = \texttt{match}\ \Box\ \texttt{with} \left|\begin{array}{l} \sigma_1\ x_1 \rightarrow C[\sigma_1\ x_1] \\ \sigma_2\ x_2 \rightarrow C[\sigma_2\ x_2] \end{array}\right.$$

η for natural numbers sounds very difficult!

Positives in richer systems?

η for sums:

$$C[\Box : A + B] = \texttt{match}\ \Box\ \texttt{with}\ \left|\ \begin{array}{l} \sigma_1\ x_1 \to C[\sigma_1\ x_1] \\ \sigma_2\ x_2 \to C[\sigma_2\ x_2] \end{array}\right.$$

η for natural numbers sounds very difficult!

$$C[\Box : \mathbb{N}] = \mathrm{rec}(\Box, t_0, D_1)$$

$$\begin{array}{l} C \circ S = D_1 \circ H \\ C \circ 0 = t_0 \end{array}$$

Arbob Ahmad, Daniel R. Licata, and Robert Harper. Deciding coproduct equality with focusing. Online draft, 2010.

Thorsten Altenkirch and Tarmo Uustalu. Normalization by evaluation for lambda^{-2}. In **FLOPS**, 2004.

Jean-Marc Andreoli. Logic Programming with Focusing Proof in Linear Logic. **Journal of Logic and Computation**, 2(3), 1992.

Taus Brock-Nannestad and Carsten Schürmann. Focused natural deduction. In **LPAR-17**, 2010.

Kaustuv Chaudhuri, Dale Miller, and Alexis Saurin. Canonical sequent proofs via multi-focusing. In **IFIP TCS**, 2008.

Guillaume Munch-Maccagnoni. **Syntax and Models of a non-Associative Composition of Programs and Proofs**. PhD thesis, Univ. Paris Diderot, 2013.

Gabriel Scherer. **Which types have a unique inhabitant? Focusing on pure program equivalence.** PhD thesis, Université Paris-Diderot, 2016.

Gabriel Scherer. Deciding equivalence with sums and the empty type. In **POPL**, 2017.

Noam Zeilberger. **The Logical Basis of Evaluation Order and Pattern-Matching**. PhD thesis, Carnegie Mellon University, 2009.