Normalization by Evaluation for Sized Dependent Types

Andreas Abel[1] Andrea Vezzosi[1] Theo Winterhalter[2]

[1]Department of Computer Science and Engineering
Chalmers and Gothenburg University, Sweden

[2]Université de Nantes, France

The European Network on Types for Programming and Verification
(EUTYPES)
Working Group meeting
24 January 2018

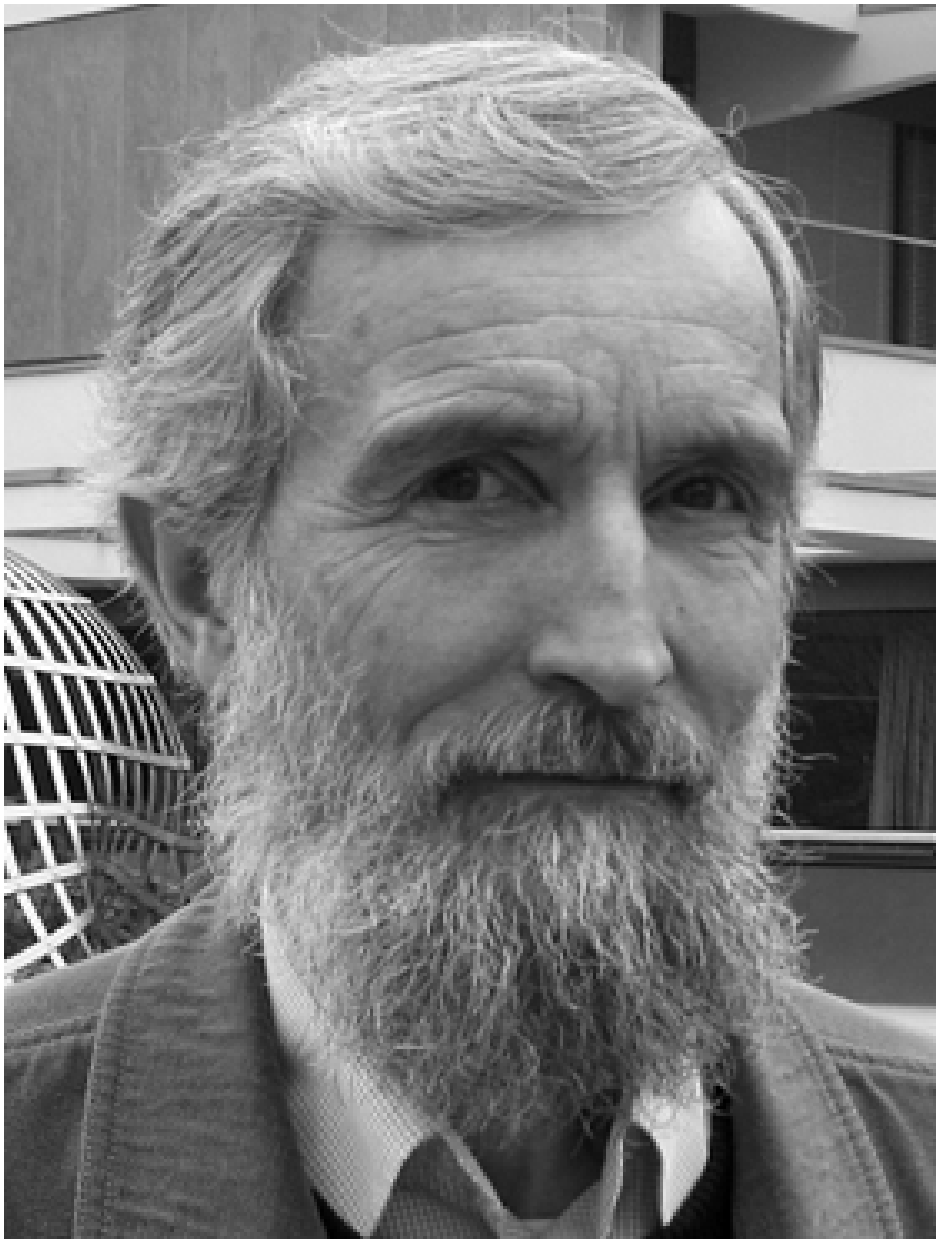
Dependent type theory à la Martin-Löf

- Typing judgement $\Gamma \vdash t : A$
  - in context Γ, expression t has type A
  - under hypotheses Γ, term t is a proof of proposition A
- Consistency: empty type not inhabited $\not\vdash t : \bot$.
- Conversion / subsumption rule

$$\frac{\Gamma \vdash t : A \qquad \Gamma \vdash A \leq B}{\Gamma \vdash t : B}$$

- Definitional equality $\Gamma \vdash t = t' : A$
  in Γ, terms t and t' of type A are not distinguished
- Reflexivity rule of subtyping

$$\frac{\Gamma \vdash A = B : \mathrm{Type}}{\Gamma \vdash A \leq B}$$



Subtyping??

Definitional equality

- Decidable (for type checking).
- Proper subrelation of extensional equality (usually $\not\vdash x + y = y + x$).
- Equates at least computationally equal terms.
- The bigger, the better!
- Type needed for η-laws, e.g., for unit type $\top$.

$$\frac{\Gamma \vdash t : \top \qquad \Gamma \vdash t' : \top}{\Gamma \vdash t = t' : \top}$$

Sized types as refinement types

- Termination needed for consistency.
  $\mathsf{fix} : ((\mathsf{Nat} \to C) \to (\mathsf{Nat} \to C)) \to \mathsf{Nat} \to C$ inconsistent
- Index data types by tree height: "$\mathsf{Nat}^{\,i} = \{n \mid n < i\}$"
  $\mathsf{fix} : (\forall i \to (\mathsf{Nat}^{\,i} \to C) \to (\mathsf{Nat}^{\,i+1} \to C)) \to \forall i \to \mathsf{Nat}^{\,i} \to C$
- Polymorphism $t : (\forall i \to \mathsf{Tree}^i \to \mathsf{Tree}^i) \to \forall i \to \mathsf{Tree}^i \to \mathsf{Tree}^\infty$
- Subtyping: $\mathsf{Nat}^{\,0} \leq \mathsf{Nat}^{\,1} \leq \mathsf{Nat}^{\,2} \leq \cdots \leq \mathsf{Nat}^{\,\infty}$
- Size expressions are not unique. Problematic for proofs.

$$\begin{array}{lcl} \mathsf{suc} & : & \forall i \to \mathsf{Nat}^{\,i} \to \mathsf{Nat}^{\,i+1} \\ \mathsf{suc}\, i & : & \mathsf{Nat}^{\,i} \to \mathsf{Nat}^{\,\infty} \\ \mathsf{suc}\,(i+1) & : & \mathsf{Nat}^{\,i} \to \mathsf{Nat}^{\,\infty} \\ \mathsf{suc}\,\infty & : & \mathsf{Nat}^{\,i} \to \mathsf{Nat}^{\,\infty} \end{array}$$

- Intuition: Sizes are *irrelevant* in terms, but *relevant* in types.

Grau ist alle Theorie

Agda demo

Church-style vs. Curry style

- Pure Type Systems: Church-style
  dependent functions = polymorphic functions.

$$\frac{\Gamma \vdash t = t' : (i : \mathsf{Size}) \to A \qquad \Gamma \vdash b : \mathsf{Size}}{\Gamma \vdash t\, b = t'\, b : A[b/i]}$$

- Curry-style would fit our needs:

$$\frac{\Gamma \vdash t = t' : \forall i{:}\mathsf{Size}.\, A \qquad \Gamma \vdash b : \mathsf{Size}}{\Gamma \vdash t = t' : A[b/i]}$$

- Absent size arguments cannot spoil our proofs.
- Synthesis: *Churry-style*.

Church-style vs. Curry style

- Pure Type Systems: Church-style
  dependent functions = polymorphic functions.

$$\frac{\Gamma \vdash t = t' : (i : \mathsf{Size}) \to A \qquad \Gamma \vdash b : \mathsf{Size}}{\Gamma \vdash t\, b = t'\, b : A[b/i]}$$

- Curry-style would fit our needs:

$$\frac{\Gamma \vdash t = t' : \forall i{:}\mathsf{Size}.\, A \qquad \Gamma \vdash b : \mathsf{Size}}{\Gamma \vdash t = t' : A[b/i]}$$

- Absent size arguments cannot spoil our proofs.
- Synthesis: *Churry-style*.

"Churry-style"

- Use size arguments for *type checking*.
- Ignore them during *equality checking*.
- Irrelevant size quantification:

$$\frac{\Gamma \vdash t = t' : (\bullet i : \mathsf{Size}) \to A \qquad \Gamma \vdash a, a', b : \mathsf{Size}}{\Gamma \vdash t\,\langle a \rangle = t'\,\langle a' \rangle : A[b/i]}$$

- Forces to ignore arguments also during *typing*.

$$\frac{\Gamma \vdash t : (\bullet i : \mathsf{Size}) \to A \qquad \Gamma \vdash a, b : \mathsf{Size}}{\Gamma \vdash t\,\langle a \rangle : A[b/i]}$$

- (Bidirectional) *type checking*:

$$\frac{\Gamma \vdash t \rightrightarrows (\bullet i : \mathsf{Size}) \to A \qquad \Gamma \vdash a \leftleftarrows \mathsf{Size}}{\Gamma \vdash t\,\langle a \rangle \rightrightarrows A[a/i]}$$

Does "Churry-style" work in general?

- Generally, can we have?

$$\frac{\Gamma \vdash t = t' : (\bullet x : A) \to B \qquad \Gamma \vdash u, u', v : A}{\Gamma \vdash t\,\langle u \rangle = t'\,\langle u' \rangle : B[v/x]}$$

- Not with type-directed η!

$$\frac{\vdash f : (\bullet X : \mathsf{Type}) \to (X \to X) \to C}{\begin{array}{l} \vdash f\langle A \to A\rangle(\lambda xy \to x\,y) \\ = f\langle A \to \top\rangle(\lambda xy \to \_) \\ = f\langle A \to A\rangle(\lambda xy \to x\,(x\,y)) \end{array}}$$

- In $(\bullet x : A) \to B$, the *shape* of B must be independent of x.
  - Same shape: $\mathsf{Nat}^{\,i}$, $\mathsf{Nat}^{\,j+1}$, $\mathsf{Nat}^{\,\infty}$.
  - Different shape: $\top$, $\bot$, $A \to B$.

Shape-irrelevance

- These are shape-irrelevant in i

$$\bullet\bullet i \vdash \mathsf{Nat}^{\,i}$$
$$\bullet\bullet i \vdash \mathsf{Nat}^{\,i} \to \mathsf{Nat}^{\,i+1}$$
$$\bullet\bullet i \vdash \mathsf{if}\ b\ \mathsf{then}\ \mathsf{Nat}^{\,i}\ \mathsf{else}\ \mathsf{Nat}^{\,i} \to \mathsf{Nat}^{\,i}$$
$$\bullet\bullet i \vdash (x : \mathsf{Nat}^{\,i}) \to \mathsf{Vec}\,A\,x$$

- These are *not* shape-irrelevant:

$$\bullet\bullet b : \mathsf{Bool} \not\vdash \mathsf{if}\ b\ \mathsf{then}\ \mathsf{Type}\ \mathsf{else}\ \mathsf{Type} \to \mathsf{Type}$$
$$\bullet\bullet X : \mathsf{Type} \not\vdash X$$
$$\bullet\bullet X : \mathsf{Type} \not\vdash X \to X$$

Official rules for irrelevant quantifier

- Formation:

$$\frac{\Gamma \vdash A : \mathsf{Type} \qquad \Gamma, \bullet\bullet x : A \vdash B : \mathsf{Type}}{\Gamma \vdash (\bullet x : A) \to B : \mathsf{Type}}$$

- Introduction:

$$\frac{\Gamma, \bullet x : A \vdash t : B}{\Gamma \vdash (\lambda x \to t) : (\bullet x : A) \to B}$$

- Elimination:

$$\frac{\Gamma \vdash t : (\bullet x : A) \to B \qquad \bullet^{-1}(\Gamma) \vdash u, v : A}{\Gamma \vdash t\, u : B[v/x]}$$

- *Resurrection* $\bullet^{-1}(\Gamma)$ removes $\bullet$s. (Nuyts et al.: $\bullet \setminus \Gamma$)

Defining Shapes (in the Model)

- Base types of the same shape:

$$\mathbf{1} \approx \mathbf{1} \qquad \mathsf{Nat}^{\,i} \approx \mathsf{Nat}^{\,j} \qquad \mathsf{Set}_{\ell} \approx \mathsf{Set}_{\ell'}$$

- Function types:

$$\frac{A_1 \approx A_2 \qquad B_1(a) \approx B_2(a) \text{ for all } a \in A_1}{(x : A_1) \to B_1(x) \approx (x : A_2) \to B_2(x)}$$

- *Not symmetric!*

$$\mathit{template} \sqsubseteq \mathit{shape}$$

- No syntactic judgement for *same shape*. :(

Finally, Normalization by Evaluation (NbE)!

- TA-NbE (TA = Type Assignment)
- Values a are (extended) weak head normal forms.
- Relations $a \in A$ and $a = a' \in A$ between whnfs.
- Reflecting neutral term u as value $\uparrow^A u \in A$:

$$\begin{array}{rcl} (\uparrow^{(x:A)\to B(x)} u)(a) & = & \uparrow^{B(a)} (u \downarrow^A a) \\ (\uparrow^{(\bullet x:A)\to B(x)} u)(a) & = & \uparrow^{B(a)} (u \langle \downarrow^A a \rangle) \end{array}$$

- Reifying value $a \in A$ as normal term $\downarrow^A a$:

$$\begin{array}{rcl} \downarrow^{\mathbf{1}} a & = & \star \\ \downarrow^{(x:A)\to B(x)} f & = & \lambda y. \downarrow^{B(\uparrow^A y)} f(\uparrow^A y) \end{array}$$

Reflection and Reification

Theorem

Let $A \lesssim A_1$ and $A \lesssim A_2$.

1. *If u_1 and u_2 are equal neutrals then $\uparrow^{A_1} u_1 = \uparrow^{A_2} u_2 \in A$.*
2. *If $a_1 = a_2 \in A$ then $\downarrow^{A_1} a_1$ and $\downarrow^{A_2} a_2$ are equal normal forms.*

Proof.

- Goal $\uparrow^{(\bullet x:A_1)\to B_1(x)} u_1 = \uparrow^{(\bullet x:A_2)\to B_2(x)} u_2 \in (\bullet x : A) \to B(x)$.
- Assume $a_1 \in A$ and $a_2 \in A$.
- Show $(\uparrow^{(\bullet x:A_1)\to B_1(x)} u_1)(a_1) = (\uparrow^{(\bullet x:A_2)\to B_2(x)} u_2)(a_2) \in B(a_1)$.
- Show $\uparrow^{B_1(a_1)}(u_1\langle\downarrow^{A_1} a_1\rangle) = \uparrow^{B_2(a_2)}(u_2\langle\downarrow^{A_2} a_2\rangle) \in B(a_1)$.

Since $B_1(x)$ and $B_2(x)$ are shape-irrelevant in x, we apply the induction hypothesis with $B(a_1) \lesssim B_1(a_1)$ and $B(a_1) \lesssim B_2(a_2)$. □

Decidability

- NbE decides definitional equality.
- Type checking (bidirectional) decidable with rule:

$$\frac{\Gamma \vdash t \rightrightarrows (\bullet x : U) \to T(x) \qquad \bullet^{-1}(\Gamma) \vdash u : U}{\Gamma \vdash t\langle u \rangle \rightrightarrows T(u)}$$

Take home message

The irrelevance modality allows us to ignore sizes where they just help the type checker.

$$\mathsf{suc}\langle \mathit{ignoreMe} \rangle\, n \;:\; \mathsf{Nat}^{\,\mathit{dontIgnoreMe}}$$

Future work

- Explore *shape-irrelevance*.
- Replace NbE by traditional algorithmic equality.
- Solidify Agda implementation of shape-irrelevance.