Algorithmic Equality for the Calculus of Constructions

Andreas Abel

Department of Computer Science
Ludwig-Maximilians-University Munich

Two Days on the Models of the Calculus of Constructions
INRIA pi.r2, Paris
14 February 2011

The Calculus of Constructions

- Full PTS (pure type system) over sorts $s ::= * \mid \Box$.

$$\frac{}{\Gamma \vdash * : \Box} \qquad \frac{\Gamma, x:U \vdash T : s}{\Gamma \vdash \Pi\, U\, (\lambda x T) : s}$$

$$\frac{\Gamma, x:U \vdash t : T}{\Gamma \vdash \lambda x{:}U.\, t : T} \qquad \frac{\Gamma \vdash t : \Pi\, U\, T \qquad \Gamma \vdash u : U}{\Gamma \vdash t\, u : T\, u}$$

$$\frac{\Gamma \vdash t : T \qquad \text{“}T = U\text{”}}{\Gamma \vdash t : U}$$

- Write $(x:U) \to T$ for $\Pi\, U\, \lambda x T$.

Metatheory of the Calculus of Constructions

- Deciding type checking.
- Main issue: deciding definitional equality.
- To handle η for unit types, need typed equality.

$$\Gamma \vdash t = t' : T$$

- Hard problem: *injectivity* of function type constructor.

$$\Gamma \vdash (x : U) \to T = (x : U') \to T' : *$$
$$\text{implies } \Gamma \vdash U = U' : * \text{ and } \Gamma \vdash T = T' : *$$

Algorithmic Equality

- Bidirectional type-directed equality à la Harper/Pfenning (2005).

$$\frac{}{\Gamma \vdash t \Longleftrightarrow t' : 1} \qquad \frac{\Gamma, x:U \vdash t\,x \Longleftrightarrow t'\,x : T}{\Gamma \vdash t \Longleftrightarrow t' : (x:U) \to T}$$

$$\frac{\Gamma \vdash n \longleftrightarrow n' : (x:U) \to T \qquad \Gamma \vdash u \Longleftrightarrow u' : U}{\Gamma \vdash n\,u \longleftrightarrow n'\,u' : T[u/x]}$$

- Type equality:

$$\frac{\Gamma \vdash U \Longleftrightarrow U' \qquad \Gamma, x:U \vdash T \Longleftrightarrow T'}{\Gamma \vdash (x:U) \to T \Longleftrightarrow (x:U') \to T'}$$

- Algorithmic equality yields injectivity.
- Assymetric choice technical problem in meta-theory.
  (cf. Untyped equality: need confluence to show normalization.)

Meta-Theoretic Results

NORM Normalization.

SR Subject reduction.

SALEQ Soundness of algorithmic equality.

$$\Gamma \vdash t \iff t' : T \text{ implies } \Gamma \vdash t = t' : T$$

CALEQ Completeness of algorithmic equality (opposite direction).

TALEQ Termination of algorithmic equality.

DECEQ Decidability of equality.

DEC Decidability of type checking.

DISCR Discrimination $0 \neq 1$.

INJ Injectivity.

CON Consistency.

Proving Meta-Theoretic Results

- Dependencies of Meta-Theorems:

$$
\begin{array}{lcl}
\text{SR} & \Longrightarrow & \text{SALEQ} \\
\text{NORM} & \Longrightarrow & \text{TALEQ} \\
\text{SALEQ} + \text{CALEQ} + \text{TALEQ} & \Longleftrightarrow & \text{DECEQ} \\
\text{DEQEQ} & \Longrightarrow & \text{DEC} \\
\text{CALEQ} & \Longrightarrow & \text{DISCR} \\
\text{CALEQ} + \text{SALEQ} & \Longrightarrow & \text{INJ} \\
\text{NORM} + \text{DISCR} & \Longrightarrow & \text{CON}
\end{array}
$$

- Build a model that verifies SR, NORM, and CALEQ.
  (cf. Goguen's TOS (1994): SR + NORM + CONFL)

Transitivity of Algorithmic Equality

- Krike-model for CALEQ ...

$$\Gamma \vdash t = t' : T \text{ implies } (t, t') \in [\![T]\!]\Gamma \text{ implies } \Gamma \vdash t \iff t' : T$$

- ... fails for lack of transitivity:

$$\frac{\Gamma \vdash n_1 \longleftrightarrow n_2 : (x:U) \to T \qquad \Gamma \vdash u_1 \iff u_2 : U}{\Gamma \vdash n_1\, u_1 \longleftrightarrow n_2\, u_2 : T[u_1/x]}$$

$$\frac{\Gamma \vdash n_2 \longleftrightarrow n_3 : (x:U') \to T' \qquad \Gamma \vdash u_2 \iff u_3 : U'}{\Gamma \vdash n_2\, u_2 \longleftrightarrow n_3\, u_3 : T'[u_2/x]}$$

- $(x:U) \to T$ and $(x:U') \to T'$ are not identical!
- $\Gamma \vdash n_1\, u_1 \longleftrightarrow n_3\, u_3 : T[u_1/x]$ requires SALEQ and INJ.

Heterogeneous Equality

- Let each term carry its own type and context!

$$\frac{\begin{array}{rcl}\Gamma_1 \vdash n_1 : (x:U_1) \to T_1 & \longleftrightarrow & \Gamma_2 \vdash n_2 : (x:U_2) \to T_2 \\ \Gamma_1 \vdash u_1 : U_1 & \Longleftrightarrow & \Gamma_2 \vdash u_2 : U_2\end{array}}{\Gamma_1 \vdash n_1\, u_1 : T_1[u_1/x] \longleftrightarrow \Gamma_2 \vdash n_2\, u_2 : T_2[u_2/x]}$$

$$\frac{\begin{array}{rcl}\Gamma_2 \vdash n_2 : (x:U_2) \to T_2 & \longleftrightarrow & \Gamma_3 \vdash n_3 : (x:U_3) \to T_3 \\ \Gamma_2 \vdash u_2 : U_2 & \Longleftrightarrow & \Gamma_3 \vdash u_3 : U_3\end{array}}{\Gamma_2 \vdash n_2\, u_2 : T_2[u_2/x] \longleftrightarrow \Gamma_3 \vdash n_3\, u_3 : T_3[u_3/x]}$$

- Transitivity now a trivial induction.

Pairing Expressions

- Consider pairs $p, q, P, Q ::= (p_1, p_2)$ of expressions.

Pair expr.	Meaning
$*$	$(*, *)$
$\Box$	$(\Box, \Box)$
$(x : P) \to Q$	$((x : P_1) \to Q_1,\ (x : P_2) \to Q_2)$
x	(x, x)
$\lambda x : P.\, q$	$(\lambda x : P_1.\, q_1,\ \lambda x : P_2.\, q_2)$
$q\, p$	$(q_1\, p_1,\ q_2\, p_2)$
$q[p/x]$	$(q_1[p_1/x], q_2[p_2/x])$
$\Psi, x : P$	$((\Psi_1, x : P_1),\ (\Psi_2, x : P_2))$

- Pairs of contexts $\Psi ::= (\Psi_1, \Psi_2)$ where $\mathrm{dom}(\Psi_1) = \mathrm{dom}(\Psi_2)$.

Algorithmic-Equality in Pair-Notation

- $\downarrow t$ computes weak head normal form of t.
- Type-directed equality.

$$\frac{\Psi, x:P \vdash t\,x \Longleftrightarrow t'\,x : \downarrow Q}{\Psi \vdash t \Longleftrightarrow t' : (x:P) \to Q} \qquad \frac{\Psi \vdash \downarrow t \longleftrightarrow \downarrow t' : \_}{\Psi \vdash t \Longleftrightarrow t' : (N, N')}$$

- Structural equality of neutrals.

$$\frac{}{\Psi \vdash x \longleftrightarrow x : \downarrow \Psi(x)}$$

$$\frac{\Psi \vdash n \longleftrightarrow n' : (x:P) \to Q \qquad \Psi \vdash t \Longleftrightarrow t' : \downarrow P}{\Psi \vdash n\,t \longleftrightarrow n'\,t' : \downarrow (Q[(t,t')/x])}$$

Algorithmic-Equality in Pair-Notation II

- Type-equality.

$$\frac{}{\Psi \vdash * \Longleftrightarrow * : \Box} \qquad \frac{\Psi \vdash N \longleftrightarrow N' : \_}{\Psi \vdash N \Longleftrightarrow N' : s}$$

$$\frac{\Psi \vdash \downarrow U \Longleftrightarrow \downarrow U' : s \qquad \Psi, x:(U, U') \vdash \downarrow T \Longleftrightarrow \downarrow T' : s'}{\Psi \vdash (x:U) \to T \Longleftrightarrow (x:U') \to T' : s'}$$

Equality in Pair-Notation

- Algorithmic equality judgements.

$$\Psi \vdash n_1 \longleftrightarrow n_2 : P \qquad \text{structural equality (neutrals)}$$
$$\Psi \vdash t_1 \Longleftrightarrow t_2 : P \qquad \text{type-directed equality}$$
$$\Psi \vdash T_1 \Longleftrightarrow T_2 : s \qquad \text{type equality}$$

- Declarative equality judgement.

$$\Psi \vdash t_1 = t_2 : P \qquad \text{heterogeneous definitional equality}$$

- Combination:

$$\begin{aligned}
\mathrm{tm}(P)_\Psi &= \{(t, t') \mid \Psi_1 \vdash t : P_1 \text{ and } \Psi_2 \vdash t' : P_2\} \\
\overline{\mathrm{eq}}(P)_\Psi &= \{(t, t') \mid \Psi \vdash t = t' : P \text{ and } \Psi \vdash t \Longleftrightarrow t' : P\} \\
\underline{\mathrm{eq}}(P)_\Psi &= \{(n, n') \mid \Psi \vdash n = n' : P \text{ and } \Psi \vdash n \longleftrightarrow n' : P\}
\end{aligned}$$

Functions and Equality

- Application (function elimination) preserves neutrality:

$$\frac{q \in \underline{\mathrm{eq}}((x:P) \to Q)_\Psi \qquad p \in \overline{\mathrm{eq}}(P)_\Psi}{q\,p \in \underline{\mathrm{eq}}(Q[p/x])_\Psi}$$

- We write $\Phi \leq \Psi$ if Φ extends Ψ.
- Abstraction (function introduction): Let $q \in \mathrm{tm}((x:P) \to Q)_\Psi$.

$$\frac{\forall \Phi \leq \Psi, p \in \underline{\mathrm{eq}}(P)_\Phi.\ q\,p \in \overline{\mathrm{eq}}(Q[p/x])_\Phi}{q \in \overline{\mathrm{eq}}((x:P) \to Q)_\Psi}$$

- Proof: consider $\Phi = \Psi, x:P$ and $p = x$. From $q_1\,x = q_2\,x$ follows $\lambda x:P_1.\,q_1\,x = \lambda x:P_2.\,q_2\,x$, thus $q_1 = q_2$ by η.

Stratification

- CoC lets us easily distinguish *terms*, *types*, and *kinds*.
- Simple kinds $k, l ::= \diamond \mid * \mid k \longrightarrow l$.
  1. $P^{\diamond}$ means P is a type (containing terms).
  2. P^{*} means P is base kind $*$ (containing types).
  3. $P^{k \to l}$ means P is a higher kind $(x : Q^{k}) \longrightarrow R^{l}$ (containing type constructors).

Expression	Interpretation	*Set*-Component
Term t	$(\mathrm{whnf}(t), ())$	nothing
Type T	$(\mathrm{whnf}(T), \mathcal{A})$	Kripke-PER $\mathcal{A}$ on term interpretations
Ty.Constr. T	$(\mathrm{whnf}(T), \mathcal{F})$	Operator $\mathcal{F}$ on Kripke-PERs
Kind $*$	$(*, [\![*]\!])$	Kripke-PER $[\![*]\!]$ on type interprations
Higher kind K	$(\mathrm{whnf}(K), \mathcal{K})$	Kripke-PER $\mathcal{K}$ on operators

Applicative Structure

- Write $t \cdot u$ for weak head normalizing $t\,u$.
- Yields a partial applicative structure on weak head normal forms.
- Partial applicative structure on semantic values:

$$\begin{array}{lcl} (t, ()) \cdot (u, \mathcal{G}) & = & (t \cdot u,\ ()) \\ (t, \mathcal{F}) \cdot (u, \mathcal{G}) & = & (t \cdot u,\ \mathcal{F}(u, \mathcal{G})) \end{array}$$

- Extension $d \cdot e$ to pairs $d = ((t_1, \mathcal{F}_1), (t_2, \mathcal{F}_2))$ of semantic values:

$$d \cdot e = (d_1 \cdot e_1,\ d_2 \cdot e_2)$$

PERs are Groupoids

- A Partial Equivalence Relation (PER) is a groupoid of pairs with:

$$\begin{array}{lcll} (a, a')^{-1} & = & (a', a) & \text{symmetry} \\ (a_1, a_2) \circ (a_2, a_3) & = & (a_1, a_3) & \text{transitivity} \end{array}$$

- If $\mathcal{A}$ is a groupoid, a *family* $\mathcal{F} : \mathcal{A} \to S$ be a map from $\mathcal{A}$ into some set S with

$$\begin{array}{lcl} \mathcal{F}(p^{-1}) & = & \mathcal{F}(p) \\ \mathcal{F}(p \circ q) & = & \mathcal{F}(p) \quad = \quad \mathcal{F}(q). \end{array}$$

Semantic Types

- If $T : K^k$ then the set-interpretation of T lives in $\langle k \rangle$.

$$
\begin{array}{lcll}
\langle \diamond \rangle & = & \{()\} & \text{unit type} \\
\mathrm{Per}(X) & = & \mathcal{P}((\mathrm{Exp} \times X)^2) & \text{PERs} \\
\mathrm{KPer}(X) & = & \mathrm{Cxt}^2 \to \mathrm{Per}(X) & \text{Kripke PERs} \\
\langle * \rangle & = & \mathrm{KPer}(\langle \diamond \rangle) & \text{KPERs of terms} \\
\langle k \to l \rangle & = & (\mathrm{Exp} \times \langle k \rangle)^2 \rightharpoonup \langle l \rangle & \text{Operators}
\end{array}
$$

- Raw semantics $\mathrm{sem}(P)^k \in \mathrm{KPer}(\langle k \rangle)$:

$$
\begin{array}{rcl}
\mathrm{sem}(P)^k_\Psi & = & \{((t, \mathcal{F}), (t', \mathcal{F}')) \mid (t, t') \in \mathrm{tm}(P)_\Psi \\
& & \qquad \text{and } \mathcal{F} = \mathcal{F}' \in \langle k \rangle\}.
\end{array}
$$

- The actual semantics of P will be subset of $\mathrm{sem}(P)^k_\Psi$.

Kripke Function Space

- If $\mathcal{K} \in \mathrm{KPer}(\langle k \rangle)$ and $\mathcal{L}_\Phi : \mathcal{K}_\Phi \to \mathrm{Per}(\langle l \rangle)$, then

$$\begin{array}{rcl}(\prod^{(x:P^k)\to Q^l} \mathcal{K}\,\mathcal{L})_\Psi & = & \{f \in \mathrm{sem}((x:P) \to Q)^{k\to l}_\Psi \mid \\ & & \quad \forall \Phi \le \Psi, g \in \mathcal{K}_\Phi.\ f \cdot g \in \mathcal{L}_\Phi(g)\} \\ & \in & \mathrm{Per}(\langle k \to l \rangle)\end{array}$$

- P^k *realizes* $\mathcal{K}$, written $\mathcal{P} \Vdash^k \mathcal{K}$, if for all Φ,

$$\underline{P^k_\Phi} \subseteq \mathcal{K}_\Phi \subseteq \overline{P}^k_\Phi$$

- Goal: function space is realized.

$$\frac{\begin{array}{c}\underline{P^k_\Psi} \subseteq \mathcal{K}_\Psi \subseteq \overline{P}^k_\Psi \\ \forall \Phi \le \Psi, d \in \mathcal{K}_\Phi.\ \underline{Q[d/x]^l_\Phi} \subseteq \mathcal{L}_\Psi(d) \subseteq \overline{Q[d/x]}^l_\Phi\end{array}}{\underline{(x:P) \to Q^{k\to l}_\Psi} \subseteq (\prod^{(x:P^k)\to Q^l} \mathcal{K}\,\mathcal{L})_\Psi \subseteq \overline{(x:P) \to Q}^{k\to l}_\Psi}$$

Candidate Space

- Define $\overline{P}^k$ and $\underline{P}^k$ by induction on k.

$$\begin{array}{lcl}
\overline{P}^{\diamond}_{\Psi} & = & \{((t,()),(t',()) \mid (t,t') \in \overline{\mathrm{eq}}(P)_{\Psi}\} \\
\underline{P}^{\diamond}_{\Psi} & = & \{((n,()),(n',()) \mid (n,n') \in \underline{\mathrm{eq}}(P)_{\Psi}\}
\end{array}$$

$$\begin{array}{lcl}
\overline{P}^{*}_{\Psi} & = & \{((Q_1,\mathcal{A}),(Q_2,\mathcal{A})) \mid Q \in \overline{\mathrm{eq}}(P)_{\Psi} \text{ and } Q \Vdash^{\diamond} \mathcal{A}\} \\
\underline{P}^{*}_{\Psi} & = & \{((Q_1,\mathcal{A}),(Q_2,\mathcal{A})) \mid Q \in \underline{\mathrm{eq}}(P)_{\Psi} \text{ and } \mathcal{A} = \underline{Q}^{\diamond}\}
\end{array}$$

$$\begin{array}{lcl}
\overline{(x:P) \to Q}^{k \to l} & = & \prod \underline{P}^k\,(d \mapsto \overline{Q[d/x]}^{l}) \\
\underline{(x:P) \to Q}^{k \to l} & = & \prod \overline{P}^k\,(d \mapsto \underline{Q[d/x]}^{l})
\end{array}$$

- Candidates $\mathcal{K}$ are realized Kripke PERs,

$$\underline{P}^k_{\Psi} \subseteq \mathcal{K}_{\Psi} \subseteq \overline{P}^k_{\Psi}.$$

Consequences

- NORM + SR: If $\Gamma \vdash t : T$ then

$$(\!|(t,t)|\!) \in [\![(T,T)]\!]_{(\Gamma,\Gamma)}$$

  implying t has whnf v and $\Gamma \vdash t = v : T$.
- CALEG: If $\Psi \vdash p_1 = p_2 : P^k$ then

$$(\!|p|\!) \in [\![P]\!]_\Psi \subseteq \overline{P}^k_\Psi$$

  hence, $p \in \overline{\mathsf{eq}}(P)_\Psi$ and $\Psi \vdash p_1 \mathrel{\widehat{\Longleftrightarrow}} p_2 : P$.
- DECEQ, DEC, DISCR, INJ, and CON follow.

Conclusions

- Kripke-style *universal* model of CoC.
- One model for the whole meta-theory.
- Accomodates inductive types in $*$ and η for unit types.
- Types in $*$ can be defined by recursion (large/strong eliminations).
- Need induction on simple kinds.
- Future work: scale to predicative hierarchy and CIC.
- Related: Coquand/Gallier (1991), Werner (1992), Goguen (1994), Barras (1997).