Blame and coercion: together again for the first time (PLDI 2015)

Jeremy Siek (Indiana)
Peter Thiemann (Freiburg)
Philip Wadler (Edinburgh)

WG 2.8, Keffalonia, 25–29 May 2015

Part I

Conclusion

Three calcluli

- $\lambda\mathsf{B}$ Blame calculus
  Findler and Felleisen (2002)
  Wadler and Findler (2009)
- $\lambda\mathsf{C}$ Coercion calculus
  Henglein (1994)
- $\lambda\mathsf{S}$ Space-efficient coercion calculus
  Hermann, Tomb, Flanagan (2007)
  Siek and Wadler (2010)
  Garcia (2013)

Full abstraction

Strong correctness property: Full abstraction

- $M \stackrel{\mathsf{ctx}}{=}_{\mathsf{B}} N$ if and only if $|M|^{\mathsf{BC}} \stackrel{\mathsf{ctx}}{=}_{\mathsf{C}} |N|^{\mathsf{BC}}$
- $M \stackrel{\mathsf{ctx}}{=}_{\mathsf{C}} N$ if and only if $|M|^{\mathsf{CS}} \stackrel{\mathsf{ctx}}{=}_{\mathsf{T}} |N|^{\mathsf{CS}}$

Equivalences in $\lambda\mathsf{B}$ and $\lambda\mathsf{C}$ easily proved in $\lambda\mathsf{S}$

Key lemma

Fundamental property of casts

Four subtyping relations: $<:$ $\quad <:^{+}$ $\quad <:^{-}$ $\quad <:_{n}$

Translation between $\lambda\mathsf{B}$ and $\lambda\mathsf{C}$ explains $<:^{+}$ and $<:^{-}$

Part II

The Blame Calculus (λB)

Types and ground types

Base types	ι		
Types	A, B, C	$::=$	$\iota \mid A \to B \mid \star$
Ground types	G, H	$::=$	$\iota \mid \star \to \star$

$$\star \;=\; \iota + (\star \to \star)$$

Compatibility

$$\frac{\Gamma \vdash M : A \qquad A \sim B}{\Gamma \vdash (M : A \stackrel{p}{\Longrightarrow} B) : B}$$

$$\frac{}{A \sim \star} \qquad \frac{}{\star \sim A} \qquad \frac{}{\iota \sim \iota} \qquad \frac{A' \sim A \qquad B \sim B'}{A \to B \sim A' \to B'}$$

Lemma 1. *If* $A \neq \star$ *then there is a unique* G *such that* $A \sim G$.

Lemma 2. $\sim$ *is reflexive and symmetric but not transitive.*

Reductions

$$\mathcal{E}[V : \iota \stackrel{p}{\Longrightarrow} \iota] \longrightarrow \mathcal{E}[V]$$

$$\mathcal{E}[(V : A \to B \stackrel{p}{\Longrightarrow} A' \to B')\ W] \longrightarrow$$

$$\mathcal{E}[(V\ (W : A' \stackrel{\bar{p}}{\Longrightarrow} A)) : B \stackrel{p}{\Longrightarrow} B']$$

$$\mathcal{E}[V : \star \stackrel{p}{\Longrightarrow} \star] \longrightarrow \mathcal{E}[V]$$

$$\mathcal{E}[V : A \stackrel{p}{\Longrightarrow} \star] \longrightarrow \mathcal{E}[V : A \stackrel{p}{\Longrightarrow} G \stackrel{p}{\Longrightarrow} \star]$$

$$\text{if } A \neq \star,\ A \neq G,\ A \sim G$$

$$\mathcal{E}[V : \star \stackrel{p}{\Longrightarrow} A] \longrightarrow \mathcal{E}[V : \star \stackrel{p}{\Longrightarrow} G \stackrel{p}{\Longrightarrow} A]$$

$$\text{if } A \neq \star,\ A \neq G,\ A \sim G$$

$$\mathcal{E}[V : G \stackrel{p}{\Longrightarrow} \star \stackrel{q}{\Longrightarrow} G] \longrightarrow \mathcal{E}[V]$$

$$\mathcal{E}[V : G \stackrel{p}{\Longrightarrow} \star \stackrel{q}{\Longrightarrow} H] \longrightarrow \mathtt{blame}\ q \qquad \text{if } G \neq H$$

Part III

The Coercion Calculus (λC)

Coercions and typing

$$\frac{}{\mathtt{id}_A : A \Longrightarrow A}$$

$$\frac{}{G\,\mathtt{!} : G \Longrightarrow \star} \qquad \frac{}{\mathtt{?}^p G : \star \Longrightarrow G}$$

$$\frac{c : A' \Longrightarrow A \qquad d : B \Longrightarrow B'}{c \to d : A \to B \Longrightarrow A' \to B'}$$

$$\frac{c : A \Longrightarrow B \qquad d : B \Longrightarrow C}{c\,;d : A \Longrightarrow C}$$

$$\frac{A \neq \star \qquad A \sim G \qquad G \neq H}{\perp^{GpH} : A \Longrightarrow B}$$

Failure

$$\frac{A \neq \star \qquad A \sim G \qquad G \neq H}{\perp^{GpH} : A \Longrightarrow B}$$

$\perp^{GpH} : A \Longrightarrow B$ corresponds to

$$M : A \xRightarrow{\bullet} G \xRightarrow{\bullet} \star \xRightarrow{p} H \xRightarrow{\bullet} B$$

Lemma 3. *(Failure) If $A \neq \star$ and $A \sim G$ and $G \neq H$ then*

$$M : A \xRightarrow{p_1} G \xRightarrow{p_2} \star \xRightarrow{p_3} H \xRightarrow{p_4} B \quad \longrightarrow \quad \texttt{blame}\ p_3\ .$$

Reductions

$$
\begin{aligned}
\mathcal{E}[V\langle \mathtt{id}_A\rangle] &\longrightarrow \mathcal{E}[V] \\
\mathcal{E}[(V\langle c \to d\rangle)\ W] &\longrightarrow \mathcal{E}[(V\ (W\langle c\rangle))\langle d\rangle] \\
\mathcal{E}[V\langle G\,\mathtt{!}\rangle\langle \mathtt{?}^p G\rangle] &\longrightarrow \mathcal{E}[V] \\
\mathcal{E}[V\langle G\,\mathtt{!}\rangle\langle \mathtt{?}^p H\rangle] &\longrightarrow \mathtt{blame}\ p & \text{if } G \neq H \\
\mathcal{E}[V\langle c\,;d\rangle] &\longrightarrow \mathcal{E}[V\langle c\rangle\langle d\rangle] \\
\mathcal{E}[V\langle \perp^{GpH}\rangle] &\longrightarrow \mathtt{blame}\ p
\end{aligned}
$$

Part IV

Space-efficient Blame Calculus (λS)

Coercions in normal form

Space-efficient coercions	s, t	$::=$	$\mathtt{id}_\star \mid ?^p G\,; i \mid i$
Intermediate coercions	i	$::=$	$g\,; G\,! \mid g \mid \bot^{GpH}$
Ground coercions	g, h	$::=$	$\mathtt{id}_\iota \mid s \to t$

Lemma 4.

- *If* $i : A \Longrightarrow B$ *then* $A \neq \star$.
- *If* $g : A \Longrightarrow B$ *then* $A \neq \star$ *and* $B \neq \star$, *and there is a unique* G *such that* $A \sim G$ *and* $B \sim G$.

Space-efficient composition

$$\mathtt{id}_\iota \mathbin{;} \mathtt{id}_\iota = \mathtt{id}_\iota$$

$$(s \rightarrow t) \mathbin{;} (s' \rightarrow t') = (s' \mathbin{;} s) \rightarrow (t \mathbin{;} t')$$

$$\mathtt{id}_\star \mathbin{;} t = t$$

$$(g \,;\, G\,!) \mathbin{;} \mathtt{id}_\star = g \,;\, G\,!$$

$$(?^p G \,;\, i) \mathbin{;} t = \; ?^p G \,;\, (i \mathbin{;} t)$$

$$g \mathbin{;} (h \,;\, H\,!) = (g \mathbin{;} h) \,;\, H\,!$$

$$(g \,;\, G\,!) \mathbin{;} (?^p G \,;\, i) = g \mathbin{;} i$$

$$(g \,;\, G\,!) \mathbin{;} (?^p H \,;\, i) = \bot^{GpH} \qquad \text{if } G \neq H$$

$$\bot^{GpH} \mathbin{;} s = \bot^{GpH}$$

$$g \mathbin{;} \bot^{GpH} = \bot^{GpH}$$

Reductions

$$\begin{aligned}
\mathcal{F}[U\langle \mathtt{id}_\iota\rangle] &\longrightarrow \mathcal{F}[U] \\
\mathcal{E}[(U\langle s \to t\rangle)\ W] &\longrightarrow \mathcal{E}[(U\ (W\langle s\rangle))\langle t\rangle] \\
\mathcal{F}[U\langle \mathtt{id}_\star\rangle] &\longrightarrow \mathcal{F}[U] \\
\mathcal{F}[M\langle s\rangle\langle t\rangle] &\longrightarrow \mathcal{F}[M\langle s\,;\,t\rangle] \\
\mathcal{F}[U\langle \perp^{GpH}\rangle] &\longrightarrow \mathtt{blame}\ p
\end{aligned}$$

Compare: Herman, Tomb, and Flanagan (2007)

$$\mathcal{F}[M\langle c\rangle\langle d\rangle] \longrightarrow \mathcal{F}[M\langle c\,;d\rangle]$$

$$(c\,;d)\,;e = c\,;(d\,;e)$$

$$\mathtt{id}_A\,;c = c$$

$$c\,;\mathtt{id}_A = c$$

$$(c \to d)\,;(c' \to d') = (c'\,;c) \to (d\,;d')$$

$$G\,\mathtt{!}\,;\mathtt{?}G = \mathtt{id}_G$$

$$G\,\mathtt{!}\,;\mathtt{?}H = \bot \quad \text{if } G \neq H$$

$$\bot\,;c = \bot$$

$$c\,;\bot = \bot$$

Compare: Siek and Wadler (2010)

$$\iota^{l} \mathbin{;} \iota^{m} = \iota^{l}$$

$$(P \rightarrow^{l} Q) \mathbin{;} (P' \rightarrow^{m} Q') = (P' \mathbin{;} P) \rightarrow^{l} (Q \mathbin{;} Q')$$

$$\star \mathbin{;} P = P$$

$$P \mathbin{;} \star = P$$

$$P^{G^m} \mathbin{;} Q^{H^p} = \perp^{pG^m} \quad \text{if } G \neq H$$

$$\perp^{pG^m} \mathbin{;} Q = \perp^{pG^m}$$

$$P^{G^l} \mathbin{;} \perp^{pG^m} = \perp^{pG^l}$$

$$P^{G^l} \mathbin{;} \perp^{pH^q} = \perp^{qG^l} \quad \text{if } G \neq H$$

Compare: Siek and Wadler (2010)

P^{G^l} means $P \sim G$ and the top-level blame label in P is l. If there is no top-level blame label in P, then l is ϵ.

$$
\begin{array}{rcl}
\iota^\epsilon & \text{corresponds to} & \mathtt{id}_\iota \\
\iota^p & \text{corresponds to} & \mathtt{?}^p\iota\,;\,\mathtt{id}_\iota \\
P \rightarrow^\epsilon Q & \text{corresponds to} & P \rightarrow Q \\
P \rightarrow^p Q & \text{corresponds to} & \mathtt{?}^p(\star \rightarrow \star)\,;\,(P \rightarrow Q) \\
\star & \text{corresponds to} & \mathtt{id}_\star \\
\perp^{pG^\epsilon} & \text{corresponds to} & \perp^{GpH} \\
\perp^{pG^q} & \text{corresponds to} & \mathtt{?}^q G\,;\,\perp^{GpH}
\end{array}
$$

Compare: Garcia (2013)

$$\mathcal{N}[\![\mathtt{id}_\star]\!] = \mathtt{id}_\star$$

$$\mathcal{N}[\![\mathtt{id}_\iota]\!] = \mathtt{id}_\iota$$

$$\mathcal{N}[\![\bot^{pG}]\!] = \bot^{p}$$

$$\mathcal{N}[\![\bot^{pGq}]\!] = ?^{q}G \,;\, \bot^{p}$$

$$\mathcal{N}[\![G\,!]\!] = G\,!$$

$$\mathcal{N}[\![G\,?^{p}]\!] = ?^{p}G$$

$$\mathcal{N}[\![G\,?^{p}\,!]\!] = ?^{p}G \,;\, G\,!$$

$$\mathcal{N}[\![\ddot{c}_1 \longrightarrow \ddot{c}_2]\!] = \mathcal{N}[\![\ddot{c}_1]\!] \longrightarrow \mathcal{N}[\![\ddot{c}_2]\!]$$

$$\mathcal{N}[\![\ddot{c}_1 \longrightarrow !\ \ddot{c}_2]\!] = (\mathcal{N}[\![\ddot{c}_1]\!] \longrightarrow \mathcal{N}[\![\ddot{c}_2]\!]) \,;\, (\star \longrightarrow \star)\,!$$

$$\mathcal{N}[\![\ddot{c}_1\ ?^{p}\!\longrightarrow \ddot{c}_2]\!] = ?^{p}(\star \longrightarrow \star) \,;\, (\mathcal{N}[\![\ddot{c}_1]\!] \longrightarrow \mathcal{N}[\![\ddot{c}_2]\!])$$

$$\mathcal{N}[\![\ddot{c}_1\ ?^{p}\!\longrightarrow !\ \ddot{c}_2]\!] = ?^{p}(\star \longrightarrow \star) \,;\, (\mathcal{N}[\![\ddot{c}_1]\!] \longrightarrow \mathcal{N}[\![\ddot{c}_2]\!]) \,;\, (\star \longrightarrow \star)\,!$$

Part V

Full abstraction

Contextual equivalence

Definition 5 (Contextual equivalence)**.** *Two terms are contextually equivalent, written* $M \stackrel{\mathsf{ctx}}{=}_{\mathsf{B}} N$*, if for any context* $\mathcal{C}$*, either*

1. *both converge to a value,*
   $\mathcal{C}[M] \longrightarrow^*_{\mathsf{B}} V$ *and* $\mathcal{C}[N] \longrightarrow^*_{\mathsf{B}} W$*,*
   for some values V *and* W*.*

2. *both allocate blame to the same label,*
   $\mathcal{C}[M] \longrightarrow^*_{\mathsf{B}} \texttt{blame}\ p$ *and* $\mathcal{C}[N] \longrightarrow^*_{B} \texttt{blame}\ p$*,*
   for some label p*, or*

3. *both diverge,*
   $\mathcal{C}[M]\Uparrow_{\mathsf{B}}$ *and* $\mathcal{C}[N]\Uparrow_{\mathsf{B}}$*.*

The same definition applies, mutatis mutandis, for λC and λS.

Full abstraction

The best previous result (Siek and Wadler (2010)):

Theorem 6 (Contextual equivalence without the context)**.**

- $M{\Uparrow}_{\mathsf{B}}$ *if and only if* $|M|^{\mathsf{BT}}{\Uparrow}_{\mathsf{T}}$

Our result:

Theorem 7 (Full abstraction)**.**

- $M \overset{\mathsf{ctx}}{=}_{\mathsf{B}} N$ *if and only if* $|M|^{\mathsf{BC}} \overset{\mathsf{ctx}}{=}_{\mathsf{C}} |N|^{\mathsf{BC}}$
- $M \overset{\mathsf{ctx}}{=}_{\mathsf{C}} N$ *if and only if* $|M|^{\mathsf{CS}} \overset{\mathsf{ctx}}{=}_{\mathsf{T}} |N|^{\mathsf{CS}}$

A key lemma

Lemma 8 (Equivalences)**.** *The following hold in $\lambda\mathsf{C}$.*

1. $M\langle \mathtt{id} \rangle \stackrel{\mathsf{ctx}}{=}_{\mathsf{C}} M$
2. $M\langle c\,;d \rangle \stackrel{\mathsf{ctx}}{=}_{\mathsf{C}} M\langle c \rangle\langle d \rangle$
3. $M\langle c\,;\mathtt{id} \rangle \stackrel{\mathsf{ctx}}{=}_{\mathsf{C}} M\langle c \rangle \stackrel{\mathsf{ctx}}{=}_{\mathsf{C}} M\langle \mathtt{id}\,;c \rangle$
4. $M\langle (c \to d)\,;(c' \to d') \rangle \stackrel{\mathsf{ctx}}{=}_{\mathsf{C}} M\langle (c'\,;c) \to (d\,;d') \rangle$
5. $M\langle c \to d \rangle \stackrel{\mathsf{ctx}}{=}_{\mathsf{C}} M\langle (c \to \mathtt{id})\,;(\mathtt{id} \to d) \rangle$
6. $M\langle c \to d \rangle \stackrel{\mathsf{ctx}}{=}_{\mathsf{C}} M\langle (\mathtt{id} \to c)\,;(d \to \mathtt{id}) \rangle$

Proof. Trivial to prove using full abstraction from $\lambda\mathsf{C}$ to $\lambda\mathsf{S}$. [Tricky to prove otherwise; probably requires a custom bisimulation.] $\square$

Fundamental property of casts

Lemma 9. *If* $A \mathbin{\&} B <:_n C$ *then*

$$|A \xRightarrow{p} B|^{\mathsf{BS}} = |A \xRightarrow{p} C|^{\mathsf{BS}} \mathbin{;} |C \xRightarrow{p} B|^{\mathsf{BS}}$$

Proof. Easy induction on A, B, and C. □

Corollary 10 (Fundamental Property of Casts)**.** *Let* M *be a term of* $\lambda\mathsf{B}$*. If* $A \mathbin{\&} B <:_n C$ *then*

$$M : A \xRightarrow{p} B \stackrel{\mathsf{ctx}}{=}_{\mathsf{B}} M : A \xRightarrow{p} C \xRightarrow{p} B$$

Proof. Immediate from Lemma 4 and full abstraction for $\lambda\mathsf{C}$ and $\lambda\mathsf{S}$. [Required a custom bisimulation and six lemmas in Siek and Wadler (2010)!] □

Part VI

Conclusion

Three calcluli

- $\lambda\mathsf{B}$ Blame calculus
  Findler and Felleisen (2002)
  Wadler and Findler (2009)

- $\lambda\mathsf{C}$ Coercion calculus
  Henglein (1994)

- $\lambda\mathsf{S}$ Space-efficient coercion calculus
  Hermann, Tomb, Flanagan (2007)
  Siek and Wadler (2010)
  Garcia (2013)

Full abstraction

Strong correctness property: Full abstraction

- $M \overset{\mathsf{ctx}}{=}_{\mathsf{B}} N$ if and only if $|M|^{\mathsf{BC}} \overset{\mathsf{ctx}}{=}_{\mathsf{C}} |N|^{\mathsf{BC}}$
- $M \overset{\mathsf{ctx}}{=}_{\mathsf{C}} N$ if and only if $|M|^{\mathsf{CS}} \overset{\mathsf{ctx}}{=}_{\mathsf{T}} |N|^{\mathsf{CS}}$

Equivalences in $\lambda\mathsf{B}$ and $\lambda\mathsf{C}$ easily proved in $\lambda\mathsf{S}$

Key lemma

Fundamental property of casts

Four subtyping relations ($<:$ $\quad <:^{+}$ $\quad <:^{-}$ $\quad <:_{n}$)

Translation between $\lambda\mathsf{B}$ and $\lambda\mathsf{C}$ explains $<:^{+}$ and $<:^{-}$