λdB: Blame tracking at higher fidelity

Jakub Zalewski, James McKinna

J. Garrett Morris, *Philip Wadler*

WGT, New Orleans, Saturday 25 January 2020

Three papers

Flanagan

Hybrid type checking

POPL 2006

Wadler and Findler

Well-typed programs can't be blamed

ESOP 2009

Greenberg, Pierce, and Weyrich

Contracts made manifest

POPL 2010

Part I

Then and Now

Then: Blame safety

$$\frac{M \ \mathtt{safe}\ p \qquad A <:^{+} B}{(M : A \overset{p}{\Rightarrow} B)\ \mathtt{safe}\ p}$$

$$\frac{M \ \mathtt{safe}\ p \qquad A <:^{-} B}{(M : A \overset{\bar{p}}{\Rightarrow} B)\ \mathtt{safe}\ p}$$

$$\frac{M \ \mathtt{safe}\ p \qquad |p| \neq |q|}{(M : A \overset{q}{\Rightarrow} B)\ \mathtt{safe}\ p}$$

Then: Results

Proposition 1 (Tangram with a witness)

- $A <: B$ *iff* $A <:^{+} B$ *and* $A <:^{-} B$.
- $A <:_{n} B$ *iff* $A <:^{+} B$ *and* $B <:^{-} A$.

Proposition 2 (Blame safety preservation)

If M `safe` p *and* $M \longrightarrow N$ *then* N `safe` p.

Proposition 3 (Blame safety progress)

If M `safe` p *then* $M \neq (\texttt{blame}\ p)$.

Example

$$\mathit{Pos} \stackrel{\text{def}}{=} (x : \texttt{int})\{x > 0\}$$

$$\mathit{Nat} \stackrel{\text{def}}{=} (x : \texttt{int})\{x \geq 0\}$$

$$(2 : \texttt{int} \stackrel{p}{\Rightarrow} \mathit{Pos}) : \mathit{Pos} \stackrel{q}{\Rightarrow} \mathit{Nat}$$

$$\longrightarrow$$

$$(2 : \texttt{int} \Rrightarrow \mathit{Pos}) : \mathit{Pos} \stackrel{q}{\Rightarrow} \mathit{Nat}$$

$$\longrightarrow$$

$$2 : \texttt{int} \stackrel{q}{\Rightarrow} \mathit{Nat}$$

$$\longrightarrow$$

$$2 : \texttt{int} \Rrightarrow \mathit{Nat}$$

Counter-example

$$Pos <: Nat \qquad \texttt{int} \not<: Nat$$

$$(2 : \texttt{int} \overset{p}{\Rightarrow} Pos) : Pos \overset{q}{\Rightarrow} Nat$$

$$\longrightarrow$$

$$(2 : \texttt{int} \Rrightarrow Pos) : Pos \overset{q}{\Rightarrow} Nat$$

$$\longrightarrow$$

$$2 : \texttt{int} \overset{q}{\Rightarrow} Nat$$

$$\longrightarrow$$

$$2 : \texttt{int} \Rrightarrow Nat$$

Now: Safety

$$\frac{\Delta \vdash M \ \mathtt{safe}\ p \qquad \Delta \vdash M : A <:^{+} B}{\Delta \vdash (M : A \overset{p}{\Rightarrow} B)\ \mathtt{safe}\ p}$$

$$\frac{\Delta \vdash M \ \mathtt{safe}\ p \qquad \Delta \vdash M : A <:^{-} B}{\Delta \vdash (M : A \overset{\neg p}{\Rightarrow} B)\ \mathtt{safe}\ p}$$

$$\frac{\Delta \vdash M \ \mathtt{safe}\ p \qquad |p| \neq |q|}{\Delta \vdash (M : A \overset{q}{\Rightarrow} B)\ \mathtt{safe}\ p}$$

Now: Closed environment entailment

$$\frac{\text{for all } \sigma, (\Xi \longrightarrow^* \sigma \text{ implies } \sigma^*(P) \not\longrightarrow^* \texttt{false})}{\Xi \models P}$$

Now: Results

Conjecture 1 (Tangram with a witness)

- $V : A <: B$ *iff* $V : A <:^{+} B$ *and* $V : A <:^{-} B$.
- $V : A <:_{n} B$ *iff* $V : A <:^{+} B$ *and*
  $y = (V : A \overset{\bullet}{\Rightarrow} B) \vdash y : B <:^{-} A$.

Conjecture 2 (Blame safety preservation)

If $\Delta \vdash M \ \mathtt{safe}\, p$ *and* $M \longrightarrow N$ *then* $\Delta \vdash N \ \mathtt{safe}\, p$.

Conjecture 3 (Blame safety progress)

If $\Delta \vdash M \ \mathtt{safe}\, p$ *then* $M \neq (\mathtt{blame}\, p)$.

Part II

Environments

Environments

Environments	$\Gamma ::= \cdot \mid \Gamma,\ x : A$
Runtime Environments	$\Delta ::= \cdot \mid \Delta,\ x : A \mid \Delta,\ x : A = M \mid \Delta,\ P$
Closed Environments	$\Xi ::= \cdot \mid \Xi,\ x : A = M \mid \Xi,\ P$
Substitutions	$\sigma, \rho, \eta ::= \cdot \mid \sigma,\ x = V$

$$\Gamma \subset \Delta \supset \Xi \supset \sigma$$

Part III

Typing

Dependent functions

$$\frac{\Gamma \vdash A : \mathtt{tp} \qquad \Gamma, x : A \vdash N : B}{\Gamma \vdash (\lambda x{:}A.\, N) : (x : A) \to B}$$

$$\frac{\Gamma \vdash L : (x : A) \to B \qquad \Gamma \vdash V : A}{\Gamma \vdash L\, V : B[x := V]}$$

$$\frac{\Gamma \vdash M : A \qquad \Gamma, x : A \vdash N : B \qquad \Gamma \vdash B : \mathtt{tp}}{\Gamma \vdash (\mathtt{let}\ x = M\ \mathtt{in}\ N) : B}$$

Casts and blame

$$\frac{\Gamma \vdash M : A \qquad A \sim B \qquad \Gamma \vdash B : \mathtt{tp}}{\Gamma \vdash (M : A \overset{p}{\Rightarrow} B) : B}$$

$$\frac{\Gamma \vdash A : \mathtt{tp}}{\Gamma \vdash (\mathtt{blame}\, p) : A}$$

Runtime let and conditional

$$\frac{\Delta \vdash M : A \qquad \Delta,\, x : A = M \vdash N : B \qquad \Delta \vdash B : \mathtt{tp}}{\Delta \vdash (\mathtt{let}\ x = M\ \mathtt{in}\ N) : B}$$

$$\frac{\Delta \vdash P : \mathtt{bool} \qquad \Delta,\, P \vdash M : A \qquad \Delta,\, \neg P \vdash N : A}{\Delta \vdash (\mathtt{if}\ P\ \mathtt{then}\ M\ \mathtt{else}\ N) : A}$$

Runtime casts

$$\frac{\Xi \vdash V : G}{\Xi \vdash (V : G \Rrightarrow \bigstar) : \bigstar}$$

$$\frac{\Xi \vdash V : A \qquad \Xi, x : A \vdash P : \texttt{bool} \qquad \Xi \models P[x := V]}{\Xi \vdash (V : A \Rrightarrow (x : A)\{P\}) : (x : A)\{P\}}$$

Part IV

Reductions

Reductions

$$V : \iota \stackrel{p}{\Rightarrow} \iota \longrightarrow V$$

$$V : \star \stackrel{p}{\Rightarrow} \star \longrightarrow V$$

$$V : A \stackrel{p}{\Rightarrow} \star \longrightarrow V : A \stackrel{p}{\Rightarrow} G \Rrightarrow \star \quad \text{if } A \neq \star, A \sim G$$

$$V : G \Rrightarrow \star \stackrel{p}{\Rightarrow} A \longrightarrow V : G \stackrel{p}{\Rightarrow} A \qquad \text{if } G \sim A$$

$$V : G \Rrightarrow \star \stackrel{p}{\Rightarrow} B \longrightarrow \texttt{blame}\, p \qquad \text{if } G \not\sim A$$

$$V : A \Rrightarrow (x : A)\{P\} \stackrel{p}{\Rightarrow} B \longrightarrow V : A \stackrel{p}{\Rightarrow} B$$

$$V : A \stackrel{p}{\Rightarrow} (y : B)\{Q\} \longrightarrow$$

$$\texttt{let}\; y = (V : A \stackrel{p}{\Rightarrow} B)\; \texttt{in}$$

$$\texttt{if}\; Q\; \texttt{then}\; y : B \Rrightarrow (y : B)\{Q\}\; \texttt{else}\; \texttt{blame}\, p$$

Wrap rule

$$(\lambda x{:}A.\, N) : (x : A){\to}B \overset{p}{\Rightarrow} (y : C){\to}D \longrightarrow$$

$$\lambda y{:}C.\, \texttt{let}\ x = (y : C \overset{-p}{\Rightarrow} A)\ \texttt{in}\ (N : B \overset{p}{\Rightarrow} D)$$

Part V

Entailment and environment morphisms

Closed environment entailment

$$\frac{\text{for all } \sigma, (\Xi \longrightarrow^* \sigma \text{ implies } \sigma^*(P) \not\longrightarrow^* \texttt{false})}{\Xi \models P}$$

Context morphism

$$\frac{}{\cdot : \cdot \longrightarrow \cdot} \qquad \frac{\rho : \Xi \longrightarrow \Delta \qquad \Xi \vdash_{rt} \rho^*(V) : \rho^*(A)}{(\rho, x = \rho^*(V)) : \Xi \longrightarrow (\Delta, x : A)}$$

$$\frac{\rho : \Xi \longrightarrow \Delta \qquad \Xi \vdash_{rt} \rho^*(M) : \rho^*(A)}{(\rho, x = y) : (\Xi, y : \rho^*(A) = \rho^*(M)) \longrightarrow (\Delta, x : A = M)}$$

$$\frac{\rho : \Xi \longrightarrow \Delta \qquad \Xi \vdash_{rt} \rho^*(P) : \mathtt{bool}}{\rho : (\Xi, \rho^*(P)) \longrightarrow (\Delta, P)}$$

Closing substitution

$$\frac{\rho : \Xi \longrightarrow \Delta \qquad \Xi \longrightarrow^{*} \sigma \qquad \eta = \sigma \circ \rho}{\eta : \Delta}$$

Part VI

Subtyping with a witness

Ordinary subtyping with a witness

$\boxed{V : A <: B}$

$$V : \iota <: \iota \qquad V : \bigstar <: \bigstar \qquad \frac{V : A <: G}{V : A <: \bigstar}$$

$$\frac{V = (W : A \Rrightarrow (x : A)\{P\}) \qquad W : A <: B}{V : (x : A)\{P\} <: B}$$

$$\frac{V : A <: B \qquad y : B = (V : A \overset{\bullet}{\Rightarrow} B) \models Q}{V : A <: (y : B)\{Q\}}$$

$$\frac{\begin{array}{c} y : C \vdash y : C <: A \\ y : C, x : A = (y : C \overset{\bullet}{\Rightarrow} A) \vdash (V\ x) : B <: D \end{array}}{V : (x : A) \to B <: (y : C) \to D}$$

Positive subtyping with a witness

$\boxed{V : A <:^{+} B}$

$$V : \iota <:^{+} \iota \qquad\qquad V : A <:^{+} \bigstar$$

$$\frac{V = (W : A \Rrightarrow (x : A)\{P\}) \qquad W : A <:^{+} B}{V : (x : A)\{P\} <:^{+} B}$$

$$\frac{V : A <:^{+} B \qquad y : B = (V : A \overset{\bullet}{\Rightarrow} B) \models Q}{V : A <:^{+} (y : B)\{Q\}}$$

$$\frac{\begin{array}{c} y : C \vdash y : C <:^{-} A \\ y : C, x : A = (y : C \overset{\bullet}{\Rightarrow} A) \vdash (V\ x) : B <:^{+} D \end{array}}{V : (x : A) \to B <:^{+} (y : C) \to D}$$

Negative subtyping with a witness

$\boxed{V : A <:^- B}$

$$V : \iota <:^- \iota \qquad V : \bigstar <:^- \bigstar \qquad \frac{V : A <:^- G}{V : A <:^- B}$$

$$\frac{V = (W : A \Rrightarrow (x : A)\{P\}) \qquad W : A <:^- B}{V : (x : A)\{P\} <:^- B}$$

$$\frac{V : A <:^- B}{V : A <:^- (y : B)\{Q\}}$$

$$\frac{\begin{array}{c} y : C \vdash y : C <:^+ A \\ y : C, x : A = (y : C \overset{\bullet}{\Rightarrow} A) \vdash (V\ x) : B <:^- D \end{array}}{V : (x : A) \to B <:^- (y : C) \to D}$$

Naive subtyping with a witness

$\boxed{V : A <:_n B}$

$$V : \iota <:_n \iota \qquad\qquad V : A <:_n \bigstar$$

$$\frac{V = (W : A \Rrightarrow (x : A)\{P\}) \qquad W : A <:_n B}{V : (x : A)\{P\} <:_n B}$$

$$\frac{V : A <:_n B \qquad y : B = (V : A \overset{\bullet}{\Rightarrow} B) \models Q}{V : A <:_n (y : B)\{Q\}}$$

$$\frac{\begin{array}{c} x : A \vdash x : A <:_n C \\ y : C, x : A = (y : C \overset{\bullet}{\Rightarrow} A) \vdash (V\ x) : B <:_n D \end{array}}{V : (x : A) \to B <:_n (y : C) \to D}$$

Open subtyping with a witness

$\boxed{\Delta \vdash M : A <:^{\pm}_{n} B}$

$$\frac{\text{for all } \eta : \Delta,\ (\eta^*(M) \longrightarrow^* V \text{ implies } V : \eta^*(A) <:^{\pm}_{n} \eta^*(B))}{\Delta \vdash M : A <:^{\pm}_{n} B}$$

Part VII

Results

Safety, revisited

$$\frac{\Delta \vdash M \ \mathtt{safe}\ p \qquad \Delta \vdash M : A <:^{+} B}{\Delta \vdash (M : A \overset{p}{\Rightarrow} B)\ \mathtt{safe}\ p}$$

$$\frac{\Delta \vdash M \ \mathtt{safe}\ p \qquad \Delta \vdash M : A <:^{-} B}{\Delta \vdash (M : A \overset{\neg p}{\Rightarrow} B)\ \mathtt{safe}\ p}$$

$$\frac{\Delta \vdash M \ \mathtt{safe}\ p \qquad |p| \neq |q|}{\Delta \vdash (M : A \overset{q}{\Rightarrow} B)\ \mathtt{safe}\ p}$$

Results, revisited

Conjecture 1 (Tangram with a witness)

- $V : A <: B$ *iff* $V : A <:^{+} B$ *and* $V : A <:^{-} B$.
- $V : A <:_{n} B$ *iff* $V : A <:^{+} B$ *and*
  $y = (V : A \stackrel{\bullet}{\Rightarrow} B) \vdash y : B <:^{-} A$.

Conjecture 2 (Blame safety preservation)

If $\Delta \vdash M \ \mathtt{safe}\, p$ *and* $M \longrightarrow N$ *then* $\Delta \vdash N \ \mathtt{safe}\, p$.

Conjecture 3 (Blame safety progress)

If $\Delta \vdash M \ \mathtt{safe}\, p$ *then* $M \neq (\mathtt{blame}\, p)$.