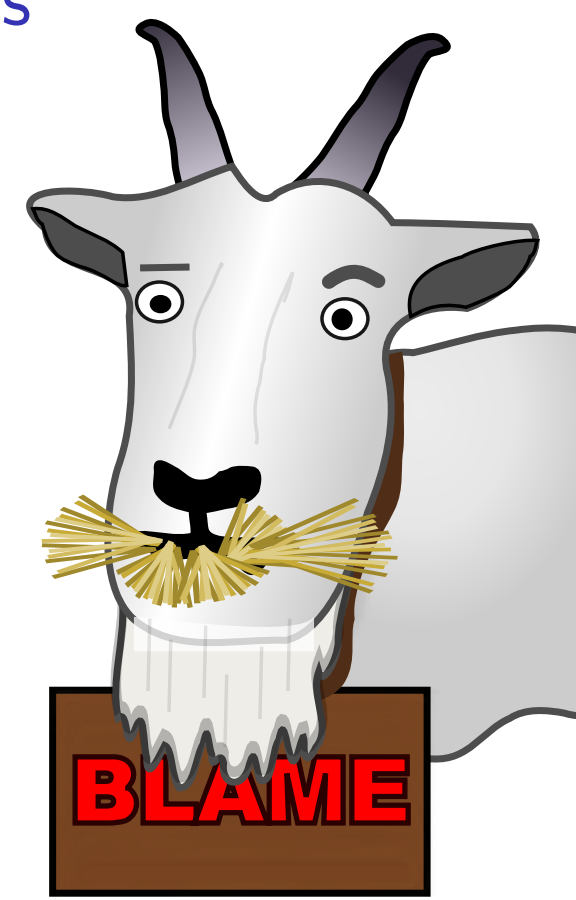
Correct Blame for Contracts

Michael Hansen

Indiana University

December 8, 2010



Contributions

- Notion of "correct" blame
  - Party that owns "bad" value and was obliged to the contract is to blame
- Tracking of ownership and obligation
- *indy* contract system
  - Contract itself can be blamed
- Addition of *indy* contracts to Racket (`->i`)
- Contract highlighter for DrRacket tool (Consigliere)
  - Highlights obligations and assumptions

Example 1

```
;; for some natural number n and real δ
(->d ([f (-> real? real?)][ε real?])
     (fp (-> real? real?))
     #:post-cond
     (for/and ([i (in-range 0 n)])
       (define x (random-number))
       (define slope
         (/ (- (f (- x ε)) (f (+ x ε)))
            (* 2 ε)))
       (<= (abs (- slope (fp x))) δ)))
```

- `random-number` may generate non-real numbers

Example 1

```
;; for some natural number n and real δ
(->d ([f (-> real? real?)][ε real?])
     (fp (-> real? real?))
     #:post-cond
     (for/and ([i (in-range 0 n)])
       (define x (random-number))
       (define slope
         (/ (- (f (- x ε)) (f (+ x ε)))
            (* 2 ε)))
       (<= (abs (- slope (fp x))) δ)))
```

- `random-number` may generate non-real numbers

```
(define random-number
  (pick-one
```



```
))
```

Syntax 'n Semantics (1/2)

Syntax

$$
\begin{array}{lrcl}
\textbf{Types} & \tau & ::= & o \mid \tau \to \tau \\
 & o & ::= & \mathit{num} \mid \mathit{bool} \\
\textbf{Terms} & e & ::= & v \mid x \mid e\ e \mid \mu x{:}\tau.e \mid e + e \\
 & & \mid & e - e \mid e \wedge e \mid e \vee e \mid \texttt{zero?}(e) \\
 & & \mid & \texttt{if}\ e\ e\ e \\
\textbf{Values} & v & ::= & 0 \mid 1 \mid -1 \mid \ldots \mid \lambda x{:}\tau.e \\
 & & \mid & \texttt{tt} \mid \texttt{ff} \\
\textbf{E. Contexts} & E & ::= & [\,] \mid E\ e \mid v\ E \mid E + e \mid v + E \\
 & & \mid & E - e \mid v - E \mid E \wedge e \mid v \wedge E \\
 & & \mid & E \vee e \mid v \vee E \mid \texttt{zero?}(E) \\
 & & \mid & \texttt{if}\ E\ e\ e
\end{array}
$$

$$
\begin{array}{lrcl}
\textbf{Contracts} & \kappa & ::= & \texttt{flat}(e) \mid \kappa \mapsto \kappa \\
\textbf{Types} & \tau & ::= & \ldots \mid \mathit{con}(\tau) \\
\textbf{Terms} & e & ::= & \ldots \mid \texttt{mon}_l^{l,l}(\kappa, e) \mid \texttt{error}^l
\end{array}
$$

$$\frac{\Gamma \vdash e : o \to \mathit{bool}}{\Gamma \vdash \texttt{flat}(e) : \mathit{con}(o)}$$

$$\frac{\Gamma \vdash \kappa_1 : \mathit{con}(\tau_1) \qquad \Gamma \vdash \kappa_2 : \mathit{con}(\tau_2)}{\Gamma \vdash \kappa_1 \mapsto \kappa_2 : \mathit{con}(\tau_1 \to \tau_2)}$$

$$\frac{\Gamma \vdash \kappa : \mathit{con}(\tau) \qquad \Gamma \vdash e : \tau}{\Gamma \vdash \texttt{mon}_j^{k,l}(\kappa, e) : \tau} \qquad \frac{}{\Gamma \vdash \texttt{error}^l : \tau}$$

Semantics

$$
\begin{array}{rrcl}
\textbf{E. Contexts} & E & ::= & \ldots \mid \texttt{mon}_l^{l,l}(\kappa, E)
\end{array}
$$

$$
\begin{array}{rcl}
E[\texttt{mon}_j^{k,l}(\kappa_1 \mapsto \kappa_2, v)] & \longmapsto & E[\lambda x.\texttt{mon}_j^{k,l}(\kappa_2, v\ \texttt{mon}_j^{l,k}(\kappa_1, x))] \\
E[\texttt{mon}_j^{k,l}(\texttt{flat}(e), v)] & \longmapsto & E[\texttt{if}\ (e\ v)\ v\ \texttt{error}^k] \\
E[\texttt{error}^l] & \longmapsto & \texttt{error}^l
\end{array}
$$

Syntax 'n Semantics (2/2)

Syntax

$$
\begin{array}{lrcl}
\textbf{Types} & \tau & ::= & o \mid \tau \to \tau \\
& o & ::= & \mathit{num} \mid \mathit{bool} \\
\textbf{Terms} & e & ::= & v \mid x \mid e\ e \mid \mu x{:}\tau.e \mid e + e \\
& & \mid & e - e \mid e \wedge e \mid e \vee e \mid \texttt{zero?}(e) \\
& & \mid & \texttt{if}\ e\ e\ e \\
\textbf{Values} & v & ::= & 0 \mid 1 \mid -1 \mid \ldots \mid \lambda x{:}\tau.e \\
& & \mid & \texttt{tt} \mid \texttt{ff} \\
\textbf{E. Contexts} & E & ::= & [\,] \mid E\ e \mid v\ E \mid E + e \mid v + E \\
& & \mid & E - e \mid v - E \mid E \wedge e \mid v \wedge E \\
& & \mid & E \vee e \mid v \vee E \mid \texttt{zero?}(E) \\
& & \mid & \texttt{if}\ E\ e\ e
\end{array}
$$

$$
\begin{array}{lrcl}
\textbf{Contracts} & \kappa & ::= & \texttt{flat}(e) \mid \kappa \mapsto \kappa \mid \kappa \overset{d}{\mapsto} (\lambda x.\kappa) \\
\textbf{Types} & \tau & ::= & \ldots \mid \mathit{con}(\tau) \\
\textbf{Terms} & e & ::= & \ldots \mid \texttt{mon}_l^{l,l}(\kappa, e) \mid \texttt{error}^l
\end{array}
$$

$$\frac{\Gamma \vdash e : o \to \mathit{bool}}{\Gamma \vdash \texttt{flat}(e) : \mathit{con}(o)}$$

$$\frac{\Gamma \vdash \kappa_1 : \mathit{con}(\tau_1) \quad \Gamma \vdash \kappa_2 : \mathit{con}(\tau_2)}{\Gamma \vdash \kappa_1 \mapsto \kappa_2 : \mathit{con}(\tau_1 \to \tau_2)}$$

$$\frac{\Gamma \vdash \kappa : \mathit{con}(\tau) \quad \Gamma \vdash e : \tau}{\Gamma \vdash \texttt{mon}_j^{k,l}(\kappa, e) : \tau} \qquad \frac{}{\Gamma \vdash \texttt{error}^l : \tau}$$

Semantics

$$\textbf{E. Contexts} \quad E ::= \ldots \mid \texttt{mon}_l^{l,l}(\kappa, E)$$

$$
\begin{array}{rcl}
E[\texttt{mon}_j^{k,l}(\kappa_1 \mapsto \kappa_2, v)] & \longrightarrow & E[\lambda x.\texttt{mon}_j^{k,l}(\kappa_2, v\ \texttt{mon}_j^{l,k}(\kappa_1, x))] \\
E[\texttt{mon}_j^{k,l}(\texttt{flat}(e), v)] & \longrightarrow & E[\texttt{if}\ (e\ v)\ v\ \texttt{error}^k] \\
E[\texttt{error}^l] & \longrightarrow & \texttt{error}^l
\end{array}
$$

$$E[\texttt{mon}_j^{k,l}(\kappa_1 \overset{d}{\mapsto} (\lambda x.\kappa_2), v)] \longrightarrow_l E[\lambda x.\texttt{mon}_j^{k,l}(\kappa_2, v\ \texttt{mon}_j^{l,k}(\kappa_1, x))] \qquad (\mathit{lax})$$

$$E[\texttt{mon}_j^{k,l}(\kappa_1 \overset{d}{\mapsto} (\lambda x.\kappa_2), v)] \longrightarrow_p E[\lambda x.\texttt{mon}_j^{k,l}(\underline{\{\texttt{mon}_j^{l,k}(\kappa_1, x)/x\}\kappa_2}, v\ \texttt{mon}_j^{l,k}(\kappa_1, x))] \qquad (\mathit{picky})$$

$$E[\texttt{mon}_j^{k,l}(\kappa_1 \overset{d}{\mapsto} (\lambda x.\kappa_2), v)] \longrightarrow_i E[\lambda x.\texttt{mon}_j^{k,l}(\underline{\{\texttt{mon}_j^{l,j}(\kappa_1, x)/x\}\kappa_2}, v\ \texttt{mon}_j^{l,k}(\kappa_1, x))] \qquad (\mathit{indy})$$

Example 2

$\Pi^1 \quad = \quad \mathtt{mon}_*^{k,l}(\kappa, \lambda f.f\ 42)\ \lambda x.x$
where $\kappa = (\mathtt{P?} \mapsto \mathtt{P?}) \overset{d}{\mapsto} (\lambda f.\mathtt{flat}(\lambda x.f\ 0 > -1))$

program	*	monitoring system	result
Π^1	—	*lax*	42
Π^1	—	*picky*	$\mathtt{error}^k$
Π^1	j	*indy*	$\mathtt{error}^j$
Π^1	k	$+$*indy*	$\mathtt{error}^k$
Π^1	l	$-$*indy*	$\mathtt{error}^l$

$\Pi^2 \quad = \quad \mathtt{mon}_*^{k,l}(\kappa, \lambda f.f\ \lambda x.x)\ \lambda g.g\ 42$
where $\kappa = ((\mathtt{P?} \mapsto \mathtt{P?}) \overset{d}{\mapsto} (\lambda f.\mathtt{flat}(\lambda x.f\ 0 > -1))) \mapsto \mathtt{P?}$

program	*	monitoring system	result
Π^2	—	*lax*	42
Π^2	—	*picky*	$\mathtt{error}^l$
Π^2	j	*indy*	$\mathtt{error}^j$
Π^2	k	$+$*indy*	$\mathtt{error}^k$
Π^2	l	$-$*indy*	$\mathtt{error}^l$

PROPOSITION 1. $e \overset{*}{\longmapsto}_i \mathtt{error}^k$ *iff* $e \overset{*}{\longmapsto}_p \mathtt{error}^{k'}$

- *picky* blames server (left) and client (right), but violation was the contract's fault!
- Intuitively, blame should follow ownership. . .

Ownership and Obligation

stacks!

Ownership

Terms $e ::= \ldots \mid \|e\|^{l} \quad \|e\|^{\overrightarrow{l_n}} \quad \|\ldots\|e\|^{l_1}\ldots\|^{l_n} \quad \|e\|^{\overleftarrow{l_n}} \quad \|\ldots\|e\|^{l_n}\ldots\|^{l_1}$

Values $v ::= \ldots \mid \|v\|^{l}$

$$\frac{\Gamma \vdash e : o \to bool}{\Gamma \vdash \lfloor \texttt{flat}(e) \rfloor^{\bar{l}} : con(o)} \qquad \frac{\Gamma \vdash e : \tau}{\Gamma \vdash \|e\|^{l} : \tau}$$

$\boxed{l \vdash e}$

$$\frac{l \vdash e_1 \quad l \vdash e_2}{l \vdash e_1\ e_2} \qquad \frac{l \vdash e}{l \vdash \lambda x.e} \qquad \frac{l \vdash e}{l \vdash \mu x.e}$$

$$\frac{l \vdash e_1 \quad l \vdash e_2 \quad l \vdash e_3}{l \vdash \texttt{if}\ e_1\ e_2\ e_3} \qquad \frac{l \vdash e_1}{l \vdash \texttt{zero?}(e_1)}$$

$$\frac{l \vdash e_1 \quad l \vdash e_2}{l \vdash e_1 + e_2} \qquad \frac{l \vdash e_1 \quad l \vdash e_2}{l \vdash e_1 - e_2}$$

$$\frac{l \vdash e_1 \quad l \vdash e_2}{l \vdash e_1 \wedge e_2} \qquad \frac{l \vdash e_1 \quad l \vdash e_2}{l \vdash e_1 \vee e_2}$$

$$\frac{}{l \vdash \texttt{n}} \qquad \frac{}{l \vdash \texttt{tt}} \qquad \frac{}{l \vdash \texttt{ff}} \qquad \frac{}{l \vdash x}$$

$$\boxed{l \vdash \texttt{mon}^{k,l}(\kappa\ \|e\|^{k})}$$

Obligation

	$((\texttt{P?} \mapsto \texttt{P?}) \overset{d}{\mapsto} (\lambda f.\texttt{flat}(\lambda x.f\ 0 > -1))) \mapsto \texttt{P?}$
server	$((\top \mapsto \texttt{P?}) \overset{d}{\mapsto} (\lambda f.\top)) \mapsto \texttt{P?}$
client	$((\texttt{P?} \mapsto \top) \overset{d}{\mapsto} (\lambda f.\texttt{flat}(\lambda x.f\ 0 > -1))) \mapsto \top$

Contracts $\kappa ::= \lfloor \texttt{flat}(\|e\|^{l}) \rfloor^{\bar{l}} \mid \kappa \mapsto \kappa \mid \kappa \overset{d}{\mapsto} (\lambda x.\kappa)$

$$\boxed{\frac{k \vdash e \qquad \{k\};\{l\};j \rhd \kappa}{l \vdash \texttt{mon}_{j}^{k,l}(\kappa, \|e\|^{k})}}$$

obligation for flat leaves

$$\frac{\bar{l};\bar{k};j \rhd \kappa_1 \qquad \bar{k};\bar{l};j \rhd \kappa_2}{\bar{k};\bar{l};j \rhd \kappa_1 \mapsto \kappa_2}$$

$$\frac{\bar{l};\bar{k} \cup \{j\};j \rhd \kappa_1 \qquad \bar{k};\bar{l};j \rhd \kappa_2}{\bar{k};\bar{l};j \rhd \kappa_1 \overset{d}{\mapsto} (\lambda x.\kappa_2)}$$

$$\frac{j \vdash e}{\bar{k};\bar{l};j \rhd \lfloor \texttt{flat}(\|e\|^{j}) \rfloor^{\bar{k}}}$$

blame follows ownership

Propagation of Ownership and Obligation

E. Contexts

$$
\begin{array}{lcl}
E^l & ::= & G^l \\
G^l & ::= & G^l\ e \mid v\ G^l \mid G^l + e \mid v + G^l \\
 & \mid & G^l - e \mid v - G^l \mid G^l \wedge e \mid v \wedge G^l \\
 & \mid & G^l \vee e \mid v \vee G^l \mid \texttt{zero?}(G^l) \\
 & \mid & \texttt{if}\ G^l\ e\ e \mid \texttt{mon}_j^{k,l}(\kappa, G^l) \\
 & \mid & \|F\|^l \mid \|G^l\|^{l'} \\
F & ::= & [\,] \mid F\ e \mid v\ F \mid F + e \mid v + F \\
 & \mid & F - e \mid v - F \mid F \wedge e \mid v \wedge F \\
 & \mid & F \vee e \mid v \vee F \mid \texttt{zero?}(F) \\
 & \mid & \texttt{if}\ F\ e\ e \mid \texttt{mon}_j^{k,l}(\kappa, F)
\end{array}
$$

$E^l[\cdots]$	$\longmapsto_m$	$E^l[\cdots]$	
$\|\mathtt{n}_1\|^{\vec{k}} + \|\mathtt{n}_2\|^{\vec{l}}$	$\cdot$	$\mathtt{n}$	where $n_1 + n_2 = n$
$\|\mathtt{n}_1\|^{\vec{k}} - \|\mathtt{n}_2\|^{\vec{l}}$	$\cdot$	$\mathtt{n}$	where $n_1 - n_2 = n$
$\texttt{zero?}(\|\mathtt{0}\|^{\vec{l}})$	$\cdot$	$\mathtt{tt}$	
$\texttt{zero?}(\|\mathtt{n}\|^{\vec{k}})$	$\cdot$	$\mathtt{ff}$	if $n \neq 0$
$\|v_1\|^{\vec{k}} \wedge \|v_2\|^{\vec{l}}$	$\cdot$	v	where $v_1 \wedge v_2 = v$
$\|v_1\|^{\vec{k}} \vee \|v_2\|^{\vec{l}}$	$\cdot$	v	where $v_1 \vee v_2 = v$
$\texttt{if}\ \|\mathtt{tt}\|^{\vec{l}}\ e_1\ e_2$	$\cdot$	e_1	
$\texttt{if}\ \|\mathtt{ff}\|^{\vec{l}}\ e_1\ e_2$	$\cdot$	e_2	
$\texttt{mon}_j^{k,l}(\kappa_1 \mapsto \kappa_2, v)$	$\cdot$	$\lambda x.\texttt{mon}_j^{k,l}(\kappa_2, v\ \texttt{mon}_j^{l,k}(\kappa_1, x))$	
$\texttt{mon}_j^{k,l}(\lfloor \texttt{flat}(e) \rfloor^{\bar{l}'}, v)$	$\cdot$	$\texttt{if}\ (e\ v)\ v\ \texttt{error}^k$	

$$E^l[\texttt{error}^k] \longmapsto_m \texttt{error}^k$$

$$E^l[\|\lambda x.e\|^{\vec{l_n}}\ v] \longmapsto_m E^l[\|\{\|v\|^{\overleftarrow{l l_n}}/x\}e\|^{\vec{l_n}}]$$

value accumulates owners

$E^l[\cdots]$	$\ldots$	$E^l[\cdots]$	
$\texttt{mon}_j^{k,l}(\kappa_1 \overset{d}{\mapsto} (\lambda x.\kappa_2), v)$	$\longmapsto_l$		
$\lambda x.\texttt{mon}_j^{k,l}(\{x/^c x\}\kappa_2, v\ \texttt{mon}_j^{l,k}(\kappa_1, x))$			*(lax)*
$\texttt{mon}_j^{k,l}(\kappa_1 \overset{d}{\mapsto} (\lambda x.\kappa_2), v)$	$\longmapsto_p$		
$\lambda x.\texttt{mon}_j^{k,l}(\{\texttt{mon}_j^{l,k}(\kappa_1, x)/^c x\}\kappa_2, v\ \texttt{mon}_j^{l,k}(\kappa_1, x))$			*(picky)*
$\texttt{mon}_j^{k,l}(\kappa_1 \overset{d}{\mapsto} (\lambda x.\kappa_2), v)$	$\longmapsto_c$		
$\lambda x.\texttt{mon}_j^{k,l}(\{\texttt{mon}_j^{l,j}(\kappa_1, x)/^c x\}\kappa_2, v\ \texttt{mon}_j^{l,k}(\kappa_1, x))$			*(indy)*

$$
\begin{array}{rcl}
\{e/^c x\}\lfloor \texttt{flat}(\|e'\|^{l'}) \rfloor^{\bar{l}} & = & \lfloor \texttt{flat}(\{\|e\|^{l'}/x\}\|e'\|^{l'}) \rfloor^{\bar{l}} \\
\{e/^c x\}\kappa_1 \mapsto \kappa_2 & = & \{e/^c x\}\kappa_1 \mapsto \{e/^c x\}\kappa_2 \\
\{e/^c x\}\kappa_1 \overset{d}{\mapsto} (\lambda x.\kappa_2) & = & \{e/^c x\}\kappa_1 \overset{d}{\mapsto} (\lambda x.\kappa_2) \\
\{e/^c x\}\kappa_1 \overset{d}{\mapsto} (\lambda y.\kappa_2) & = & \{e/^c x\}\kappa_1 \overset{d}{\mapsto} (\lambda y.\{e/^c x\}\kappa_2) \\
 & & \text{where } x \neq y
\end{array}
$$

substituted expression gets same owner

Correct Blame

DEFINITION 2 (Blame Correctness). *A contract system m is* blame correct *if for all terms e_0 such that $l_o \vdash e_0$, and*

$$e_0 \longmapsto^*_m E^\dagger[\mathtt{mon}^{k,\dagger}_\dagger(\lfloor \mathtt{flat}(e_1) \rfloor^{\bar{l}}, v)]$$

$v = \|v_1\|^k$ and $k \in \bar{l}$. The identity of the $\dagger$ labels is irrelevant.

- When a `flat` contract is checked:
  - The positive party k must be obligated to fulfill it ($k \in \bar{l}$)
  - k must own the value being checked ($v = \|v_1\|^k$)

Subject Reduction (1/3)

- Problem with well-formedness ($l \vdash e$)
  - Reduction semantics creates unsatisfactory expressions!
  - But it's only temporary, so you can relax
  - Need to generalize judgements for programs and contracts...

Subject Reduction (2/3)

$\boxed{\bar{\kappa};\bar{\iota};\iota;\Gamma \rhd \kappa}$

$$\frac{\bar{\kappa};\bar{\iota};\iota;\Gamma \rhd \lceil \mathtt{let}\, f = (\|v\|_{\iota})\, \mathtt{in}\, f \rceil_{\bar{\kappa}} \lhd \kappa \qquad \iota;\Gamma \vdash v \qquad \bar{\kappa} \subseteq \bar{\kappa}_1}{\bar{\kappa};\bar{\iota};\iota;\Gamma \rhd \kappa_1 \mapsto_{\flat} (\lambda x.\kappa_2)}$$

$$\frac{\bar{\kappa};\bar{\iota};\iota;\Gamma \rhd \kappa_1 \mapsto \kappa_2}{\bar{\iota};\bar{\kappa};\iota;\Gamma \rhd \kappa_1 \qquad \bar{\kappa};\bar{\iota};\iota;\Gamma \rhd \kappa_2}$$

$$\frac{\bar{\kappa};\bar{\iota};\iota;\Gamma \rhd \kappa \lhd \kappa \qquad \bar{\kappa};\bar{\iota};\iota;\Gamma \rhd \kappa \lhd \kappa}{\bar{\iota};\bar{\kappa} \cup \{\iota\};\iota;\Gamma \rhd \kappa}$$

$$\frac{\bar{\kappa};\bar{\iota};\iota;\Gamma \rhd \kappa \lhd \kappa}{\iota;\Gamma \vdash v \qquad \bar{\kappa} \subseteq \bar{\kappa}_1}$$

$$\frac{\Gamma(x) = \kappa \qquad \bar{\kappa};\Gamma \Vdash x}{\bar{\kappa};\Gamma \vdash x} \qquad \frac{\bar{\kappa};\Gamma \Vdash \|v\|_{\kappa} \; v_2}{\bar{\kappa};\Gamma \vdash v_1 \qquad \bar{\kappa};\Gamma \vdash v_2}$$

$$\frac{\iota;\Gamma \vdash \|v\|_{\kappa}}{\bar{\kappa};\Gamma \vdash v} \qquad \frac{\bar{\kappa};\Gamma \Vdash \|v\|_{\kappa}}{\bar{\kappa};\Gamma \vdash v} \qquad \frac{\iota;\Gamma \vdash \mathtt{mon}^{\iota}_{\kappa,\iota}(\kappa,v)}{\bar{\kappa};\Gamma \Vdash v \qquad \{\kappa\};\{\iota\};\iota;\Gamma \rhd \kappa}$$

$$\frac{\iota;\Gamma \vdash \lambda x.v}{\iota;\Gamma \uplus \{x:\iota\} \vdash v} \qquad \frac{\iota;\Gamma \vdash \mu x.v}{\iota;\Gamma / \{x\} \vdash v}$$

$\boxed{\iota;\Gamma \vdash v}$

$$\frac{}{\iota;\Gamma \vdash n} \qquad \frac{}{\iota;\Gamma \vdash ff} \qquad \frac{}{\iota;\Gamma \vdash tt} \qquad \frac{}{\iota;\Gamma \vdash x}$$

$$\frac{\iota;\Gamma \vdash v_1 \qquad \iota;\Gamma \vdash v_2}{\iota;\Gamma \vdash v_1 \wedge v_2} \qquad \frac{\iota;\Gamma \vdash v_1 \qquad \iota;\Gamma \vdash v_2}{\iota;\Gamma \vdash v_1 \vee v_2}$$

$$\frac{\iota;\Gamma \vdash v_1 \qquad \iota;\Gamma \vdash v_2}{\iota;\Gamma \vdash v_1 + v_2} \qquad \frac{\iota;\Gamma \vdash v_1 \qquad \iota;\Gamma \vdash v_2}{\iota;\Gamma \vdash v_1 - v_2}$$

$$\frac{}{\iota;\Gamma \vdash \mathtt{error}_{\kappa}} \qquad \frac{\iota;\Gamma \vdash v_1 \qquad \iota;\Gamma \vdash v_2 \qquad \iota;\Gamma \vdash v_3}{\iota;\Gamma \vdash \mathtt{if}\, v_1\, v_2\, v_3}$$

$$\frac{\iota;\Gamma \vdash v_1 \qquad \iota;\Gamma \vdash v_2}{\iota;\Gamma \vdash v_1\, v_2} \qquad \frac{\iota;\Gamma \vdash \mathtt{zero?}(v_1)}{\iota;\Gamma \vdash v_1}$$

Subject Reduction (2/3) - for real

$\boxed{j;\Gamma \vdash e}$

$$\frac{j;\Gamma \vdash e_1 \quad j;\Gamma \vdash e_2}{j;\Gamma \vdash e_1\ e_2} \qquad \frac{j;\Gamma \vdash e_1}{j;\Gamma \vdash \texttt{zero?}(e_1)}$$

$$\frac{}{j;\Gamma \vdash \texttt{error}^k} \qquad \frac{j;\Gamma \vdash e_1 \quad j;\Gamma \vdash e_2 \quad j;\Gamma \vdash e_3}{j;\Gamma \vdash \texttt{if}\ e_1\ e_2\ e_3}$$

$$\frac{j;\Gamma \vdash e_1 \quad j;\Gamma \vdash e_2}{j;\Gamma \vdash e_1 + e_2} \qquad \frac{j;\Gamma \vdash e_1 \quad j;\Gamma \vdash e_2}{j;\Gamma \vdash e_1 - e_2}$$

$$\frac{j;\Gamma \vdash e_1 \quad j;\Gamma \vdash e_2}{j;\Gamma \vdash e_1 \wedge e_2} \qquad \frac{j;\Gamma \vdash e_1 \quad j;\Gamma \vdash e_2}{j;\Gamma \vdash e_1 \vee e_2}$$

$$\frac{}{j;\Gamma \vdash \texttt{n}} \qquad \frac{}{j;\Gamma \vdash \texttt{tt}} \qquad \frac{}{j;\Gamma \vdash \texttt{ff}} \qquad \frac{}{j;\Gamma \vdash x}$$

record labels of bound variables

$$\frac{l;\Gamma \uplus \{x : l\} \vdash e}{l;\Gamma \vdash \lambda x.e} \qquad \frac{l;\Gamma \setminus \{x\} \vdash e}{l;\Gamma \vdash \mu x.e}$$

$$\frac{k;\Gamma \vdash e}{l;\Gamma \vdash \|e\|^k} \qquad \frac{k;\Gamma \vdash e}{k;\Gamma \Vdash \|e\|^k} \qquad \frac{k;\Gamma \Vdash e \quad \{k\};\{l\};j;\Gamma \rhd \kappa}{l;\Gamma \vdash \texttt{mon}_j^{k,l}(\kappa, e)}$$

$$\frac{\Gamma(x) = k}{k;\Gamma \Vdash x} \qquad \frac{k;\Gamma \vdash e_1 \quad k;\Gamma \vdash e_2}{k;\Gamma \Vdash \|e_1\|^k\ e_2}$$

free var ownership in environment

environmentally sound contract checking

$\boxed{\bar{k};\bar{l};j;\Gamma \rhd \kappa}$

$$\frac{\bar{l};\bar{k};j;\Gamma \rhd \kappa_1 \quad \bar{k};\bar{l};j;\Gamma \rhd \kappa_2}{\bar{k};\bar{l};j;\Gamma \rhd \kappa_1 \mapsto \kappa_2}$$

$$\frac{\bar{l};\bar{k} \cup \{j\};j;\Gamma \rhd \kappa_1 \quad \bar{k};\bar{l};j;\Gamma \rhd \kappa_2}{\bar{k};\bar{l};j;\Gamma \rhd \kappa_1 \overset{d}{\mapsto} (\lambda x.\kappa_2)}$$

$$\frac{j;\Gamma \vdash e \quad \bar{k} \subseteq \bar{k}'}{\bar{k};\bar{l};j;\Gamma \rhd \lfloor \texttt{flat}(\|e\|^j) \rfloor^{\bar{k}'}}$$

Subject Reduction (3/3)

PROPOSITION 4. *For all e and l, $l \vdash e$ implies $l; \varnothing \vdash e$.*

Main Theorems

THEOREM 15. $\longmapsto_l$ *and* $\longmapsto_i$ *are blame correct.*

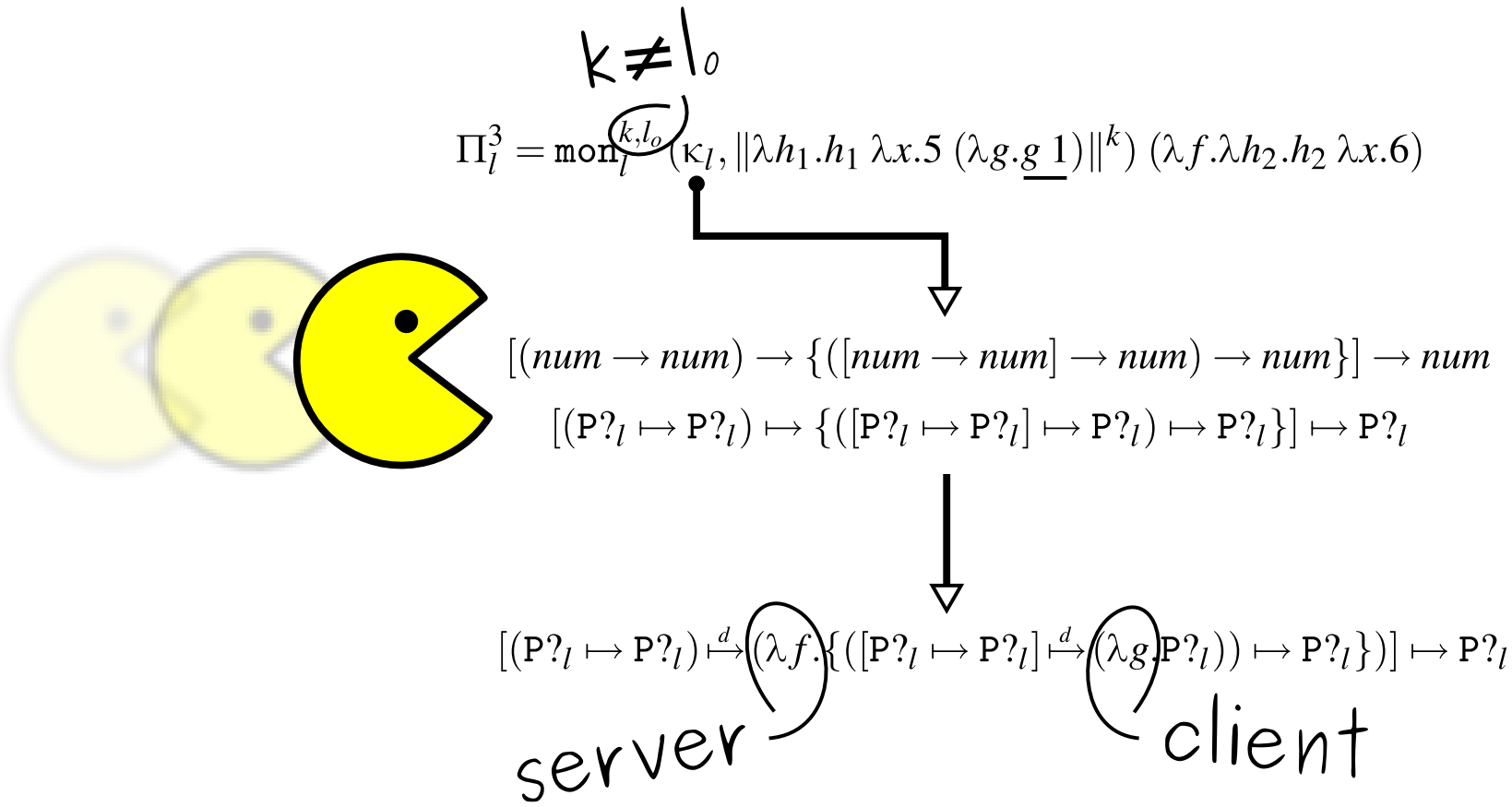
THEOREM 16. *There exists a program* e *such that* $l_o \vdash e$ *and*

$$e \overset{*}{\longmapsto}_p E^l[\mathtt{mon}_j^{k,l_2}(\lfloor \mathtt{flat}(e) \rfloor^{\bar{l}}, \|v\|^{l_1})]$$

but $k \neq l_1$.

- *lax* and *indy* are blame correct ☺
- *picky* can blame the wrong party ☹

The Setup


$k \neq l_o$
$\Pi_l^3 = \mathrm{mon}_l^{k,l_o}(\kappa_l, \|\lambda h_1.h_1\ \lambda x.5\ (\lambda g.g\ 1)\|^k)\ (\lambda f.\lambda h_2.h_2\ \lambda x.6)$
$[(num \to num) \to \{([num \to num] \to num) \to num\}] \to num$
$[(\mathrm{P}?_l \mapsto \mathrm{P}?_l) \mapsto \{([\mathrm{P}?_l \mapsto \mathrm{P}?_l] \mapsto \mathrm{P}?_l) \mapsto \mathrm{P}?_l\}] \mapsto \mathrm{P}?_l$
$[(\mathrm{P}?_l \mapsto \mathrm{P}?_l) \overset{d}{\mapsto} (\lambda f.\{([\mathrm{P}?_l \mapsto \mathrm{P}?_l] \overset{d}{\mapsto} (\lambda g.\mathrm{P}?_l)) \mapsto \mathrm{P}?_l\})] \mapsto \mathrm{P}?_l$
server
client

The Pass

$$\texttt{P?}_l \quad = \quad \texttt{flat}(\|\lambda x.x > 0\|^l)$$

$$\kappa_l \quad = \quad (((\lfloor \texttt{P?}_l \rfloor^{l_o} \mapsto \lfloor \texttt{P?}_l \rfloor^k) \overset{d}{\mapsto} (\lambda f.\kappa_l^1)) \mapsto \lfloor \texttt{P?}_l \rfloor^k$$

$$\kappa_l^1 \quad = \quad (((\lfloor \texttt{P?}_l \rfloor^k \mapsto \lfloor \texttt{P?}_l \rfloor^{l_o}) \overset{d}{\mapsto} (\lambda g.\kappa_l^2)) \mapsto \lfloor \texttt{P?}_l \rfloor^k$$

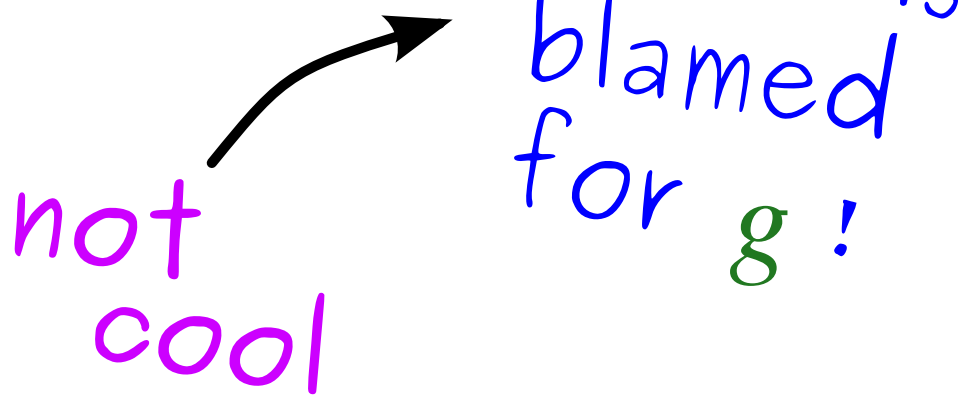
server is responsible

$$\kappa_l^2 \quad = \quad \lfloor \texttt{flat}(\|\lambda x.\texttt{zero?}(f\ 1 - g\ 0)\|^l) \rfloor^k$$

The Fumble

$$E_0^{l_o}[\mathtt{mon}_{l_o}^{l_o,k}(\lfloor \mathtt{P}?_{l_o} \rfloor^{l_o}, \|\|1\|^{l_o}\|^{l_o})] \longmapsto^{*} p$$

$$E_1^{l_o}[\mathtt{mon}_{l_o}^{k,l_o}(\lfloor \mathtt{P}?_{l_o} \rfloor^{l_o}, \|\|0\|^{l_o}\|^{l_o})]$$



Play-by-Play

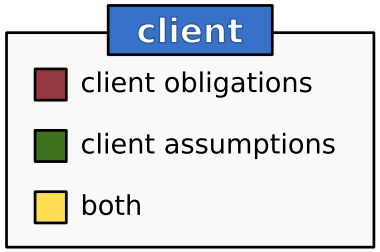
$$\lambda h_1.h_1\ \lambda x.5\ (\lambda g.g\ 1) \quad \leftarrow \quad (\lambda f.\lambda h_2.h_2\ \lambda x.6)$$

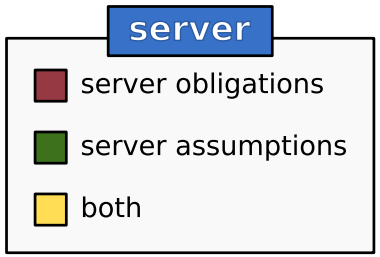
$$\kappa_1 = [(P \mapsto P) \mapsto f : \{[P \mapsto P] \mapsto g : P\}] \mapsto P$$

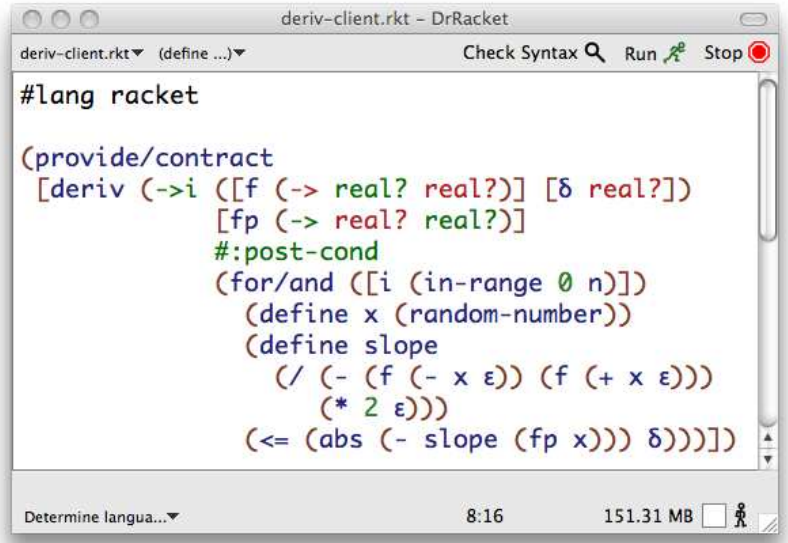
$$\ldots (f\ 1 - \underline{g\ 0}) \ldots$$

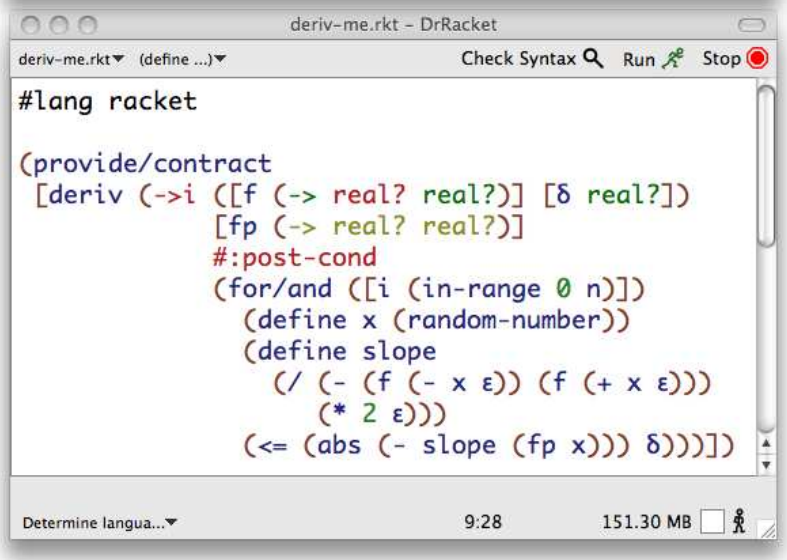
Expression	Contract
$(\lambda f.\lambda h_2.h_2\ \lambda x.6)\ \lambda x.5\ (\lambda g.g\ 1)$	$h_1 : \kappa_1$
$(\lambda h_2.h_2\ \lambda x.6)\ (\lambda g.g\ 1)$	$f = \lambda x.5 : (P \mapsto P)$
$(\lambda g.g\ 1)\ \lambda x.6$	$(\lambda g.g\ 1) : ([P \mapsto P] \mapsto P)$
$\lambda x.6$	$g = \lambda x.6 : [P \mapsto P]$

Consigliere (1/2)

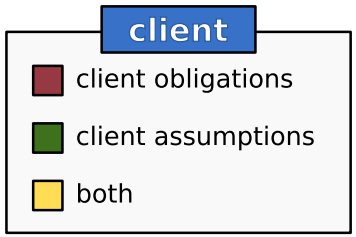


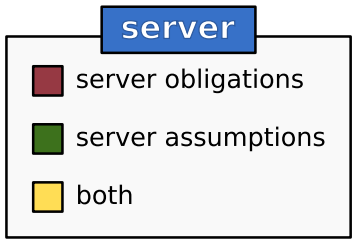


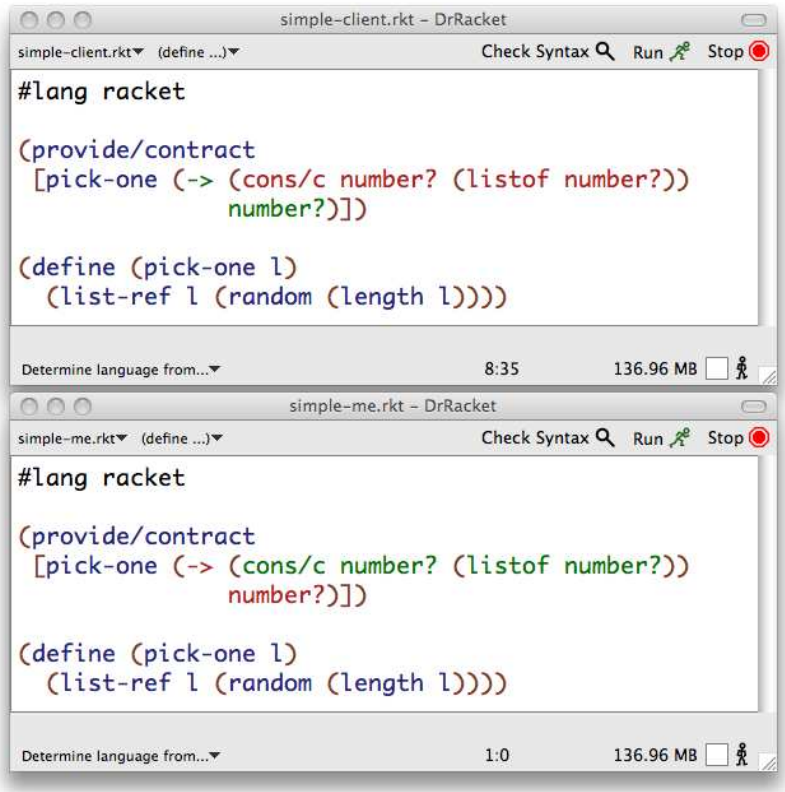




Consigliere (2/2)







Questions?