Modular Analysis via Abstract Reduction Semantics

Sam Tobin-Hochstadt and David Van Horn

Modular Analysis via Abstract Reduction Semantics

Sam Tobin-Hochstadt and David Van Horn

Not to appear at ESOP'11

Modularity matters.

Modularity of analysis matters.

Modularity matters.

- Some programs are open (c.f.: the web).

```
// dynamically load any javascript file.
load.getScript = function(filename) {
  var script = document.createElement('script')
  script.setAttribute("type","text/javascript")
  script.setAttribute("src", filename)
  if (typeof script!="undefined")
  document.getElementsByTagName("head")[0]
          .appendChild(script)
}
```

Modularity matters.

- Good components are written in bad languages.

```
#include "escheme.h"
Scheme_Object *scheme_initialize(Scheme_Env *env) {
  Scheme_Env *mod_env;
  mod_env = scheme_primitive_module(scheme_intern_symbol("hi"),
                                    env);
  scheme_add_global("greeting",
                    scheme_make_utf8_string("hello"),
                    mod_env);
  scheme_finish_primitive_module(mod_env);
  return scheme_void;
}

Scheme_Object *scheme_reload(Scheme_Env *env) {
  return scheme_initialize(env); /* Nothing special for reload */
}

Scheme_Object *scheme_module_name() {
  return scheme_intern_symbol("hi");
}
```

Modularity matters.

- Programs are big; analysis is hard.

Theorem

$$1\mathrm{MLOC} + O(n^3) = \text{☹}$$

□

Modularity matters.

- Programs are big; analysis is hard.

Theorem

$$1\mathrm{MLOC} + O(n^3) = \text{☹}$$

$$1\mathrm{KLOC} + O(2^n) = \text{☠}$$

□

Modularity matters.

- Libraries matter.

```
;; To use: (require (planet dvanhorn/ralist))
;; Purely Functional Random-Access Lists.
;; Implementation based on Okasaki, FPCA '95.
#lang racket
(provide (all-defined-out))

(struct tree        (val))
(struct (leaf tree) ())
(struct (node tree) (left right))

;; X [RaListof X] -> [RaListof X]
(define (ra:cons x ls)
 (match ls
   [(list-rest (cons s t1) (cons s t2) r)
    (cons (cons (+ 1 s s) (make-node x t1 t2)) r)]
   [else
    (cons (cons 1 (make-leaf x)) ls)]))
...
```

Semantics-based analysis matters.

$$
\begin{array}{ll}
((\lambda x^{\beta}.e)^{\ell_\lambda}\ v^{\ell_v})^{\ell_a} & \longrightarrow e[v^{\ell_v}/x^{\beta}] \\
(n^{\ell_n}\ v^{\ell_v})^{\ell_a} & \longrightarrow (\text{blame } \lambda\ \mathcal{R})^{\ell_a} \\
(\text{if0 } 0^{\ell_0}\ e_1\ e_2)^{\ell} & \longrightarrow e_1 \\
(\text{if0 } v^{\ell_v}\ e_1\ e_2)^{\ell} & \longrightarrow e_2 \\
(\text{int}_f^{\ell\ell'} \Leftarrow n^{\ell_n})^{\ell_c} & \longrightarrow n^{\ell} \\
(\text{int}_f^{\ell\ell'} \Leftarrow \vec{v}^{\ell_v})^{\ell_c} & \longrightarrow (\text{blame } f\ \mathcal{R})^{\ell'} \\
((c_1 \rightarrow c_2)_f^{\ell\ell'} \Leftarrow \vec{v}^{\ell_v})^{\ell_c} & \longrightarrow ((c_1 \hat{\rightarrow} c_2)_f^{\ell\ell'} \Leftarrow \vec{v}^{\ell_v})^{\ell_c} \\
((c_1 \rightarrow c_2)_f^{\ell\ell'} \Leftarrow n^{\ell_n})^{\ell_c} & \longrightarrow (\text{blame } f\ \mathcal{R})^{\ell'} \\
(((c_1 \hat{\rightarrow} c_2)_f^{\ell\ell'} \Leftarrow \vec{v}^{\ell_v})^{\ell_c}\ w^{\ell_w})^{\ell_a} & \longrightarrow (c_2 \Leftarrow (\vec{v}^{\ell_v}\ (c_1 \Leftarrow w^{\ell_w})^{\mathcal{L}^+(c_1)})^{\mathcal{L}^-(c_2)})^{\mathcal{L}^+(c_2)}
\end{array}
$$

Semantics-based analysis matters.

*Source**Sink*	$\text{int}_h^{\ell_5^+\ell_5^-}$	$\langle \dots e_5\ \text{int}_h^{\ell_5^+\ell_5^-}\rangle_h^{\ell_6^+\ell_6^-}$	$\text{any}_h^{\ell_5^+\ell_5^-}$	$\langle \dots e_5\ \text{any}_h^{\ell_5^+\ell_5^-}\rangle_h^{\ell_6^+\ell_6^-}$
$n_{e_1\dots}^{\ell_n}$		$\left.\begin{array}{l}\{\ell_n\}\subseteq\varphi(\ell_5^-)\\ e_1\dots\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$		$\left.\begin{array}{l}\{\ell_n\}\subseteq\varphi(\ell_5^-)\\ e_1\dots\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$
$\text{int}_f^{\ell_1^+\ell_1^-}$		$\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$		$\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$
$\langle \dots e_1\ \text{int}_f^{\ell_1^+\ell_1^-}\rangle_f^{\ell_2^+\ell_2^-}$		$\left.\begin{array}{l}\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\\ e_1\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$		$\left.\begin{array}{l}\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\\ e_1\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$
$\text{any}_f^{\ell_1^+\ell_1^-}$	$\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$			$\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$
$\langle \dots e_1\ \text{any}_f^{\ell_1^+\ell_1^-}\rangle_f^{\ell_2^+\ell_2^-}$				$\left.\begin{array}{l}\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\\ e_1\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$
$(\lambda x^{\beta}.e^{\ell})_{e_1\dots}^{\ell_\lambda}$	$\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$		$\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_5^+)\subseteq\varphi(\beta)$ $\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell)\subseteq\varphi(\ell_5^-)$ $\left.\begin{array}{l}\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\\ e_1\dots\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$	
$(c_g^{\ell_1^+\ell_1^-}\rightarrow c_f^{\ell_2^+\ell_2^-})_f^{\ell_3^+\ell_3^-}$	$\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$		$\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_5^+)\subseteq\varphi(\ell_1^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_2^+)\subseteq\varphi(\ell_5^-)$	
$\langle \dots e_3\ (c_g^{\ell_1^+\ell_1^-}\rightarrow c_f^{\ell_2^+\ell_2^-})_f^{\ell_3^+\ell_3^-}\rangle_f^{\ell_4^+\ell_4^-}$			$\left.\begin{array}{l}\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\\ e_3\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$	

*Source**Sink*	$(e^{\ell_5}\ e^{\ell_6})^{\ell_a}$	$(c_i^{\ell_7^+\ell_7^-}\rightarrow c_h^{\ell_8^+\ell_8^-})_h^{\ell_5^+\ell_5^-}$	$\langle \dots e_5\ (c_i^{\ell_7^+\ell_7^-}\rightarrow c_h^{\ell_8^+\ell_8^-})_h^{\ell_5^+\ell_5^-}\rangle_h^{\ell_6^+\ell_6^-}$
$n_{e_1\dots}^{\ell_n}$	$\{\ell_n\}\subseteq\varphi(\ell_5)\Rightarrow\{\langle\lambda,\mathcal{R}\rangle\}\subseteq\psi(\ell_a)$	$\{\ell_n\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$	
$\text{int}_f^{\ell_1^+\ell_1^-}$	$\{\ell_1^+\}\subseteq\varphi(\ell_5)\Rightarrow\{\langle\lambda,\mathcal{R}\rangle\}\subseteq\psi(\ell_a)$	$\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$	
$\langle \dots e_1\ \text{int}_f^{\ell_1^+\ell_1^-}\rangle_f^{\ell_2^+\ell_2^-}$			
$\text{any}_f^{\ell_1^+\ell_1^-}$			
$\langle \dots e_1\ \text{any}_f^{\ell_1^+\ell_1^-}\rangle_f^{\ell_2^+\ell_2^-}$			
$(\lambda x^{\beta}.e^{\ell})_{e_1\dots}^{\ell_\lambda}$	$\{\ell_\lambda\}\subseteq\varphi(\ell_5)\Rightarrow\varphi(\ell_6)\subseteq\varphi(\beta)$ $\{\ell_\lambda\}\subseteq\varphi(\ell_5)\Rightarrow\varphi(\ell)\subseteq\varphi(\ell_a)$	$\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_7^+)\subseteq\varphi(\beta)$ $\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell)\subseteq\varphi(\ell_8^-)$ $\left.\begin{array}{l}\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\\ e_1\dots\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$	
$(c_g^{\ell_1^+\ell_1^-}\rightarrow c_f^{\ell_2^+\ell_2^-})_f^{\ell_3^+\ell_3^-}$	$\{\ell_3^+\}\subseteq\varphi(\ell_5)\Rightarrow\varphi(\ell_6)\subseteq\varphi(\ell_1^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5)\Rightarrow\varphi(\ell_2^+)\subseteq\varphi(\ell_a)$	$\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_7^+)\subseteq\varphi(\ell_1^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_2^+)\subseteq\varphi(\ell_8^-)$	
$\langle \dots e_3\ (c_g^{\ell_1^+\ell_1^-}\rightarrow c_f^{\ell_2^+\ell_2^-})_f^{\ell_3^+\ell_3^-}\rangle_f^{\ell_4^+\ell_4^-}$		$\left.\begin{array}{l}\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\\ e_3\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$	

Table 1. Constraints creation for source-sink pairs.

Semantics-based analysis matters.

*Source**Sink*	$\text{int}_h^{\ell_5^+\ell_5^-}$	$\langle \dots e_5\ \text{int}_h^{\ell_5^+\ell_5^-}\rangle_h^{\ell_6^+\ell_6^-}$	$\text{any}_h^{\ell_5^+\ell_5^-}$	$\langle \dots e_5\ \text{any}_h^{\ell_5^+\ell_5^-}\rangle_h^{\ell_6^+\ell_6^-}$
$n_{e_1\dots}^{\ell_n}$		$\left.\begin{array}{l}\{\ell_n\}\subseteq\varphi(\ell_5^-)\\ e_1\dots\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$		$\left.\begin{array}{l}\{\ell_n\}\subseteq\varphi(\ell_5^-)\\ e_1\dots\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$
$\text{int}_f^{\ell_1^+\ell_1^-}$		$\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$		$\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$
$\langle \dots e_1\ \text{int}_f^{\ell_1^+\ell_1^-}\rangle_f^{\ell_2^+\ell_2^-}$		$\left.\begin{array}{l}\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\\ e_1\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$		$\left.\begin{array}{l}\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\\ e_1\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$
$\text{any}_f^{\ell_1^+\ell_1^-}$	$\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$			$\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$
$\langle \dots e_1\ \text{any}_f^{\ell_1^+\ell_1^-}\rangle_f^{\ell_2^+\ell_2^-}$				$\left.\begin{array}{l}\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\\ e_1\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$
$(\lambda x^{\beta}.e^{\ell})_{e_1\dots}^{\ell_\lambda}$	$\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$		$\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_5^+)\subseteq\varphi(\beta)$ $\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell)\subseteq\varphi(\ell_5^-)$ $\left.\begin{array}{l}\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\\ e_1\dots\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$	
$(c_g^{\ell_1^+\ell_1^-}\to c_f^{\ell_2^+\ell_2^-})_f^{\ell_3^+\ell_3^-}$	$\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$		$\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_5^+)\subseteq\varphi(\ell_1^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_2^+)\subseteq\varphi(\ell_5^-)$	
$\langle \dots e_3\ (c_g^{\ell_1^+\ell_1^-}\to c_f^{\ell_2^+\ell_2^-})_f^{\ell_3^+\ell_3^-}\rangle_f^{\ell_4^+\ell_4^-}$			$\left.\begin{array}{l}\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\\ e_3\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$	

*Source**Sink*	$(e^{\ell_5}\ e^{\ell_6})^{\ell_a}$	$(c_i^{\ell_7^+\ell_7^-}\to c_h^{\ell_8^+\ell_8^-})_h^{\ell_5^+\ell_5^-}$	$\langle \dots e_5\ (c_i^{\ell_7^+\ell_7^-}\to c_h^{\ell_8^+\ell_8^-})_h^{\ell_5^+\ell_5^-}\rangle_h^{\ell_6^+\ell_6^-}$
$n_{e_1\dots}^{\ell_n}$	$\{\ell_n\}\subseteq\varphi(\ell_5)\Rightarrow\{\langle\lambda,\mathcal{R}\rangle\}\subseteq\psi(\ell_a)$	$\{\ell_n\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$	
$\text{int}_f^{\ell_1^+\ell_1^-}$			
$\langle \dots e_1\ \text{int}_f^{\ell_1^+\ell_1^-}\rangle_f^{\ell_2^+\ell_2^-}$	$\{\ell_1^+\}\subseteq\varphi(\ell_5)\Rightarrow\{\langle\lambda,\mathcal{R}\rangle\}\subseteq\psi(\ell_a)$	$\{\ell_1^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$	
$\text{any}_f^{\ell_1^+\ell_1^-}$			
$\langle \dots e_1\ \text{any}_f^{\ell_1^+\ell_1^-}\rangle_f^{\ell_2^+\ell_2^-}$			
$(\lambda x^{\beta}.e^{\ell})_{e_1\dots}^{\ell_\lambda}$	$\{\ell_\lambda\}\subseteq\varphi(\ell_5)\Rightarrow\varphi(\ell_6)\subseteq\varphi(\beta)$ $\{\ell_\lambda\}\subseteq\varphi(\ell_5)\Rightarrow\varphi(\ell)\subseteq\varphi(\ell_a)$	$\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_7^+)\subseteq\varphi(\beta)$ $\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell)\subseteq\varphi(\ell_8^-)$ $\left.\begin{array}{l}\{\ell_\lambda\}\subseteq\varphi(\ell_5^-)\\ e_1\dots\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$	
$(c_g^{\ell_1^+\ell_1^-}\to c_f^{\ell_2^+\ell_2^-})_f^{\ell_3^+\ell_3^-}$	$\{\ell_3^+\}\subseteq\varphi(\ell_5)\Rightarrow\varphi(\ell_6)\subseteq\varphi(\ell_1^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5)\Rightarrow\varphi(\ell_2^+)\subseteq\varphi(\ell_a)$	$\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_7^+)\subseteq\varphi(\ell_1^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\Rightarrow\varphi(\ell_2^+)\subseteq\varphi(\ell_8^-)$	
$\langle \dots e_3\ (c_g^{\ell_1^+\ell_1^-}\to c_f^{\ell_2^+\ell_2^-})_f^{\ell_3^+\ell_3^-}\rangle_f^{\ell_4^+\ell_4^-}$		$\left.\begin{array}{l}\{\ell_3^+\}\subseteq\varphi(\ell_5^-)\\ e_3\not\sqsubseteq e_5\end{array}\right\}\Rightarrow\{\langle h,\mathcal{O}\rangle\}\subseteq\psi(\ell_5^-)$	

Table 1. Constraints creation for source-sink pairs.

An idea:

reduction semantics + abstract values
= *abstract* reduction semantics

An idea:

reduction semantics + abstract values
= *abstract* reduction semantics

$$(\lambda x.E)\ V \quad \triangleright \quad \{V/x\}E$$

An idea:

reduction semantics + abstract values
= *abstract* reduction semantics

$$\frac{\begin{array}{rcl}(\lambda x.E)\ V & \rhd & \{V/x\}E \\ (\lambda x.E) & : & A \to B\end{array}}{}$$

An idea:

reduction semantics + abstract values
= *abstract* reduction semantics

$$\frac{\begin{array}{rcl}(\lambda x.E)\ V & \rhd & \{V/x\}E \\ (\lambda x.E) & : & A \to B\end{array}}{(A \to B)\ V \quad \blacktriangleright \quad B}$$

```
(module fact (int -> int)
  (lambda (x)
    (if (= x 0)
        1
        (* x (fact (sub1 x))))))

(module input int 0)

(fact input)
```

$\triangleright^*$ `((lambda (x) ...) 0)`

$\triangleright^*$ `1`

```
(module fact (int -> int)
   •)
```

```
(module input int 0)

(fact input)

▶* ((int -> int) 0)
▶* int
```

```
(module fact (int -> int)
  (lambda (x)
    (if (= x 0)
        0
        (* x (fact (sub1 x))))))

(module input int •)

(fact input)
```

$\blacktriangleright^*$ `((lambda (x) ...) int)` $\blacktriangleright^*$ `(if (= int 0) 0 ...)`
$\blacktriangleright^*$ `(if bool 1 ...)`
$\blacktriangleright^*$ `1, int`

```
(module * (int int -> int) •)
(module sub1 (int -> int) •)
(module fact (int -> int)
  (lambda (x)
    (if (= x 0)
        1
        (* x (fact (sub1 x))))))

(module input int 0)

(fact input)

►* ((lambda (x) ...) 0)
►* 1
```

$$
\begin{array}{lcl}
P & = & M \ldots E \\
M & = & (\text{module } f\ T\ V) \\
E & = & x \mid f \mid V \mid (E\ E) \\
V & = & (\lambda x.E) \mid n \\
T & = & T \rightarrow T \mid \text{int}
\end{array}
$$

$$
\begin{array}{lcl}
P & = & M \ldots E \\
M & = & (\text{module } f\ T\ V) \mid (\text{module } f\ T\ \bullet) \\
E & = & x \mid f \mid V \mid (E\ E) \\
V & = & (\lambda x.E) \mid n \mid T \\
T & = & T \rightarrow T \mid \text{int}
\end{array}
$$

$$\mathcal{E}[(\lambda x.E)\ V] \ \triangleright\ \mathcal{E}[\{V/x\}E]$$

$$\mathcal{E}[(T' \to T)\ V] \ \blacktriangleright\ \mathcal{E}[T]$$

$$\mathcal{E}[(\lambda x.E)\ V] \ \triangleright\ \mathcal{E}[\{V/x\}E]$$

$$\mathcal{E}[(T' \to T)\ V] \ \blacktriangleright\ \mathcal{E}[T]$$

$$\ldots(\mathsf{module}\ f\ T\ V)\ldots\ \mathcal{E}[f] \ \triangleright\ \mathcal{E}[V]$$

$$\ldots(\mathsf{module}\ f\ T\ \bullet)\ldots\ \mathcal{E}[f] \ \blacktriangleright\ \mathcal{E}[T]$$

Abstract reduction is modular and sound, but not computable.

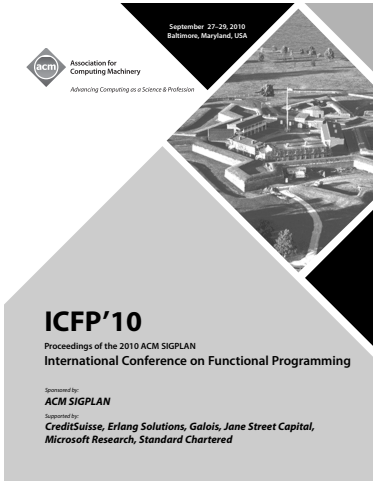
Theorem

If $P \rhd^* V$ *and* $P \sqsubseteq \widehat{P}$, *then* $\widehat{P} \blacktriangleright^* \widehat{V}$ *where* $V \sqsubseteq \widehat{V}$.

Abstract reduction composes with other approximation techniques.

Abstract reduction composes with other approximation techniques.

- Nielsen, Nielsen, and Hankin, '99
- Cousot, '02
- Van Horn and Might, '10: Abstracting Abstract Machines



Church, '36

$$\mathcal{E}[(\lambda x.E)\ V] \quad \triangleright \quad \mathcal{E}[\{V/x\}E]$$

CEK, Felleisen and Friedman, '87

$$\mathcal{E}[(\lambda x.E)\ V] \quad \triangleright \quad \mathcal{E}[\{V/x\}E]$$

$$\langle V, \rho, \mathsf{fn}((\lambda x.E), \rho', \kappa)\rangle \quad \longmapsto \quad \langle E, \rho'[x \mapsto \langle V, \rho\rangle], \kappa\rangle$$

CESK, Felleisen and Friedman, '88

$$\mathcal{E}[(\lambda x.E)\ V] \quad \rhd \quad \mathcal{E}[\{V/x\}E]$$

$$\langle V, \rho, \mathsf{fn}((\lambda x.E), \rho', \kappa)\rangle \quad \longmapsto \quad \langle E, \rho'[x \mapsto \langle V, \rho\rangle], \kappa\rangle$$

$$\langle V, \rho, \sigma, \mathsf{fn}((\lambda x.E), \rho', \kappa)\rangle \quad \longmapsto \quad \langle E, \rho'[x \mapsto b], \sigma[b \mapsto \langle V, \rho\rangle], \kappa\rangle$$

CESK*, Van Horn and Might, '10

$$\mathcal{E}[(\lambda x.E)\ V] \quad \triangleright \quad \mathcal{E}[\{V/x\}E]$$

$$\langle V, \rho, \mathsf{fn}((\lambda x.E), \rho', \kappa)\rangle \quad \longmapsto \quad \langle E, \rho'[x \mapsto \langle V, \rho\rangle], \kappa\rangle$$

$$\langle V, \rho, \sigma, \mathsf{fn}((\lambda x.E), \rho', \kappa)\rangle \quad \longmapsto \quad \langle E, \rho'[x \mapsto b], \sigma[b \mapsto \langle V, \rho\rangle], \kappa\rangle$$

$$\langle V, \rho, \sigma, a\rangle \quad \longmapsto \quad \langle E, \rho'[x \mapsto b], \sigma[b \mapsto \langle V, \rho\rangle], a'\rangle$$
$$\text{if } \sigma(a) = \mathsf{fn}((\lambda x.E), \rho', a')$$

ACESK*, Van Horn and Might, '10

$$\mathcal{E}[(\lambda x.E)\ V] \quad \triangleright \quad \mathcal{E}[\{V/x\}E]$$

$$\langle V, \rho, \mathsf{fn}((\lambda x.E), \rho', \kappa)\rangle \quad \longmapsto \quad \langle E, \rho'[x \mapsto \langle V, \rho\rangle], \kappa\rangle$$

$$\langle V, \rho, \sigma, \mathsf{fn}((\lambda x.E), \rho', \kappa)\rangle \quad \longmapsto \quad \langle E, \rho'[x \mapsto b], \sigma[b \mapsto \langle V, \rho\rangle], \kappa\rangle$$

$$\langle V, \rho, \sigma, a\rangle \quad \longmapsto \quad \langle E, \rho'[x \mapsto b], \sigma[b \mapsto \langle V, \rho\rangle], a'\rangle$$
$$\text{if } \sigma(a) = \mathsf{fn}((\lambda x.E), \rho', a')$$

$$\langle V, \rho, \hat{\sigma}, a\rangle \quad \longmapsto \quad \langle E, \rho'[x \mapsto b], \hat{\sigma} \sqcup [b \mapsto \langle V, \rho\rangle], a'\rangle$$
$$\text{if } \hat{\sigma}(a) \ni \mathsf{fn}((\lambda x.E), \rho', a')$$

$$\mathcal{E}[(T' \to T)\ V] \quad \blacktriangleright \quad \mathcal{E}[T]$$

$$\langle V, \rho, \mathsf{fn}((T' \to T), \rho', \kappa)\rangle \quad \longmapsto \quad \langle T, \emptyset, \kappa\rangle$$

$$\langle V, \rho, \sigma, \mathsf{fn}((T' \to T), \rho', \kappa)\rangle \quad \longmapsto \quad \langle T, \emptyset, \sigma, \kappa\rangle$$

$$\langle V, \rho, \sigma, a\rangle \quad \longmapsto \quad \langle T, \emptyset, \sigma, a'\rangle$$
$$\text{if } \sigma(a) = \mathsf{fn}((T' \to T), \rho', a')$$

$$\langle V, \rho, \hat{\sigma}, a\rangle \quad \longmapsto \quad \langle T, \emptyset, \hat{\sigma}, a'\rangle$$
$$\text{if } \hat{\sigma}(a) \ni \mathsf{fn}((T' \to T), \rho', a')$$

Static analyzers derived from abstract reductions semantics are modular, sound, *and computable*.

Theorem

If $S \longmapsto^*_{\text{CESK}^\star} S'$ *and* $S \sqsubseteq \widehat{S}$, *then* $\widehat{S} \longmapsto^*_{\text{ACESK}^\star} \widehat{S}'$ *where* $S' \sqsubseteq \widehat{S}'$.

$$
\begin{array}{lcl}
P & = & M \ldots E \\
M & = & (\text{module } f \ C \ V) \\
E & = & x \mid f \mid V \mid (E \ E) \mid (C \Leftarrow E) \\
V & = & (\lambda x.E) \mid n \\
C & = & C \rightarrow C \mid \text{int} \mid \text{any} \mid (\text{pred } (\lambda x.E))
\end{array}
$$

$$
\begin{array}{lcl}
P & = & M \ldots E \\
M & = & (\text{module } f\ C\ V) \mid (\text{module } f\ C\ \bullet) \\
E & = & x \mid f \mid V \mid (E\ E) \mid (C \Leftarrow E) \\
V & = & (\lambda x.E) \mid n \mid C \\
C & = & C \rightarrow C \mid \text{int} \mid \text{any} \mid (\text{pred}\ (\lambda x.E))
\end{array}
$$

$$\mathcal{E}[(\lambda x.E)\ V] \rhd \mathcal{E}[\{V/x\}E]$$

$$\mathcal{E}[(C' \to C)\ V] \blacktriangleright \mathcal{E}[C]$$

$$\mathcal{E}[(C' \to C)\ V] \blacktriangleright \text{blame } f$$

$$\mathcal{E}[(\lambda x.E)\ V] \ \triangleright\ \mathcal{E}[\{V/x\}E]$$

$$\mathcal{E}[(C' \to C)\ V] \ \blacktriangleright\ \mathcal{E}[C]$$

$$\mathcal{E}[(C' \to C)\ V] \ \blacktriangleright\ \text{blame } f$$

$$\ldots(\text{module } f\ C\ V)\ldots\ \mathcal{E}[f] \ \triangleright\ \mathcal{E}[(C \Leftarrow V)]$$

$$\ldots(\text{module } f\ C\ \bullet)\ldots\ \mathcal{E}[f] \ \blacktriangleright\ \mathcal{E}[C]$$

```
(module * (int int -> int) •)
(module sub1 (int -> int) •)
(module fact (int -> int)
  (lambda (x)
    (if (= x 0)
        1
        (* x (fact (sub1 x))))))

(module input int •)

(fact input)

►* ((lambda (x) ...) int)
►* int
```

```
(module * (any any -> int) •)
(module sub1 (any -> int) •)
(module fact any
  (lambda (x)
    (if (= x 0)
        1
        (* x (fact (sub1 x))))))

(module input int •)

(fact input)

►* ((lambda (x) ...) int)
►* int
```

```
(module input ((pred even?) -> (pred even?))
  (lambda (n) 7))

(module double (((pred even?) -> (pred even?)) ->
                ((pred even?) -> (pred even?)))
  (lambda (f)
    (lambda (x)
      (f (f x)))))

((double input) 4)
```

$\triangleright^*$ (blame input)

```
(module input ((pred even?) -> (pred even?))
  •)

(module double (((pred even?) -> (pred even?)) ->
                ((pred even?) -> (pred even?)))
  (lambda (f)
    (lambda (x)
      (f (f x)))))

((double input) 4)
```

►* (blame input), (pred even?)

```
(module input (any           -> (pred even?))
  •)

(module double ((any           -> (pred even?)) ->
                ((pred even?) -> any          ))
  (lambda (f)
    (lambda (x)
      (f (f x)))))

((double input) 4)

►* (blame input), (pred even?)
```

Related work:

- Shivers, '91, and others—modularity via black holes
- Reppy, '06—modularity via opaque signatures
- Meunier, '06—modularity via contracts

Future work:

- Analyze Racket code
- Dependent contracts
- Other specification languages

- Modularity matters.
- Semantics-based analysis matters.
- Abstract reduction semantics gives you both.

`http://bit.ly/abstract-reduction`

New England Programming Languages and Systems Symposium
Northeastern University, Boston, MA
March 4, 2011 “Spring”