Semantic Solutions to Program Analysis Problems

Sam Tobin-Hochstadt and David Van Horn

PLDI FIT 2011

A talk in three parts.

1. A provocative claim. (The thought)
2. A idea about modular program analysis. (The idea)
3. And a demo! (The fun)

The claim

Program analysis should focus on semantics

The claim

Program analysis should focus on semantics
instead of focusing on abstraction.

The claim

Program analysis should focus on semantics instead of focusing on abstraction.

$\longrightarrow$ Interesting Semantics $\longrightarrow$ Computable Analysis

The claim

Program analysis should focus on semantics instead of focusing on abstraction.

$\longrightarrow$ Interesting Semantics $\longrightarrow$ Computable Analysis

Three reasons

Why focus on semantics?

1. Semantics is easier to get right
2. Off-the-shelf approximation techniques exist
3. Semantics by itself is interesting

Getting it wrong

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

Getting it wrong

$Source \setminus Sink$	$\mathrm{int}_h^{\ell_5^+\ell_5^-}$
n^{ℓ_n}	
$\mathrm{int}_f^{\ell_1^+\ell_1^-}$	
$(\lambda x^\beta.e^\ell)^{\ell_\lambda}$	$\{\ell_\lambda\}\subseteq\varphi(\ell_5^-) \Rightarrow \{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$
$(c_g^{\ell_1^+\ell_1^-}\to c_f^{\ell_2^+\ell_2^-})_f^{\ell_3^+\ell_3^-}$	$\{\ell_3^+\}\subseteq\varphi(\ell_5^-) \Rightarrow \{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$

$Source \setminus Sink$	$(e^{\ell_5}\ e^{\ell_6})^{\ell_a}$	$(c_i^{\ell_7^+\ell_7^-}\to c_h^{\ell_8^+\ell_8^-})_h^{\ell_5^+\ell_5^-}$
n^{ℓ_n}	$\{\ell_n\}\subseteq\varphi(\ell_5) \Rightarrow \{\langle\lambda,\mathcal{R}\rangle\}\subseteq\psi(\ell_a)$	$\{\ell_n\}\subseteq\varphi(\ell_5^-) \Rightarrow \{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$
$\mathrm{int}_f^{\ell_1^+\ell_1^-}$	$\{\ell_1^+\}\subseteq\varphi(\ell_5) \Rightarrow \{\langle\lambda,\mathcal{R}\rangle\}\subseteq\psi(\ell_a)$	$\{\ell_1^+\}\subseteq\varphi(\ell_5^-) \Rightarrow \{\langle h,\mathcal{R}\rangle\}\subseteq\psi(\ell_5^-)$
$(\lambda x^\beta.e^\ell)^{\ell_\lambda}$	$\{\ell_\lambda\}\subseteq\varphi(\ell_5) \Rightarrow \varphi(\ell_6)\subseteq\varphi(\beta)$ $\{\ell_\lambda\}\subseteq\varphi(\ell_5) \Rightarrow \varphi(\ell)\subseteq\varphi(\ell_a)$	$\{\ell_\lambda\}\subseteq\varphi(\ell_5^-) \Rightarrow \varphi(\ell_7^+)\subseteq\varphi(\beta)$ $\{\ell_\lambda\}\subseteq\varphi(\ell_5^-) \Rightarrow \varphi(\ell)\subseteq\varphi(\ell_8^-)$
$(c_g^{\ell_1^+\ell_1^-}\to c_f^{\ell_2^+\ell_2^-})_f^{\ell_3^+\ell_3^-}$	$\{\ell_3^+\}\subseteq\varphi(\ell_5) \Rightarrow \varphi(\ell_6)\subseteq\varphi(\ell_1^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5) \Rightarrow \varphi(\ell_2^+)\subseteq\varphi(\ell_a)$	$\{\ell_3^+\}\subseteq\varphi(\ell_5^-) \Rightarrow \varphi(\ell_7^+)\subseteq\varphi(\ell_1^-)$ $\{\ell_3^+\}\subseteq\varphi(\ell_5^-) \Rightarrow \varphi(\ell_2^+)\subseteq\varphi(\ell_8^-)$

Getting it wrong

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

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

Table 1. Constraints creation for source-sink pairs.

Getting it wrong

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

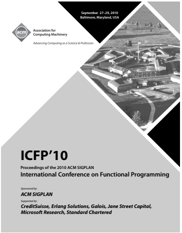
Source$\diagdown$*Sink*	$(e^{\ell_5}\ e^{\ell_6})^{\ell_a}$	$(c_i^{\ell_7^+\ell_7^-}\to c_h^{\ell_8^+\ell_8^-})_h^{\ell_5^+\ell_5^-}$	$\langle\ldots e_5\ (c_i^{\ell_7^+\ell_7^-}\to c_h^{\ell_8^+\ell_8^-})_h^{\ell_5^+\ell_5^-}\rangle_h^{\ell_6^+\ell_6^-}$
$n_{e_1\ldots}^{\ell_n}$	$\{\ell_n\}\subseteq\varphi(\ell_5)\Rightarrow\{\langle\lambda,\mathcal{R}\rangle\}\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

Table 1. Constraints creation for source-sink pairs.

The shelf

Generic abstraction techniques exist.

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



Semantics as verification

Once you have a semantics that answers interesting questions, try running it.

A Modular Semantics

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.

- 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)]))
...
```

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

$$\frac{(\lambda x.E)\ V \quad \triangleright \quad \{V/x\}E \qquad (\lambda x.E) \quad : \quad A \rightarrow B}{}$$

An idea:

reduction semantics + abstract values
= *abstract* reduction semantics

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

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

(module input int/c 0)

(fact input)
```

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

$\triangleright^*$ `1`

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

```
(module input int/c 0)

(fact input)

▶* ((int/c -> int/c) 0)
▶* int/c
```

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

(module input int/c •)

(fact input)
```

►* ((lambda (x) ...) int/c) ►* (if (= int/c 0) 0 ...)
►* (if bool 1 ...)
►* 1, int/c

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

(module input int/c 0)

(fact input)

▶* ((lambda (x) ...) 0)
▶* 1
```

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

(module input int/c •)

(fact input)

▶* ((lambda (x) ...) int/c)
▶* int/c
```

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

(module input int/c •)

(fact input)

▶* ((lambda (x) ...) int/c)
▶* int/c
```

Demo

- Focus on semantics.
- Abstract reduction provides modularity.
- A semantics can be a verifier.

`http://bit.ly/abstract-reduction`
`http://redex.racket-lang.org`