Type-based Dependency Analysis

RS^3 Topic Workshop on Concurrent Noninterference

University of Freiburg

Matthias Keil
Institute for Computer Science
Faculty of Engineering
University of Freiburg

June 2012

Notizen

Outline

University of Freiburg

Notizen

Definitions

Recap

University of Freiburg

$$
\begin{array}{llcl}
\textit{Values} & \ni v & ::= & \phi, \psi, \pi \\
\textit{Expressions} & \ni e & ::= & e(v) \mid \mathbf{if}(v)\ e
\end{array}
$$

$$e(\psi) \Downarrow \phi \tag{1.1}$$

Definition (Dependency)

$$
\begin{aligned}
&\exists \langle \psi_i, \psi_j \rangle \mid \psi_i \neq \psi_j \ : \\
&e[\psi \mapsto \psi_i] \Downarrow \phi_i \ \wedge \ e[\psi \mapsto \psi_j] \Downarrow \phi_j \ \wedge \ \phi_i \neq \phi_j \\
&\Rightarrow \ \phi \rightsquigarrow \psi
\end{aligned} \tag{1.2}
$$

Notizen

Definitions
Recap
University of Freiburg

Values	$\ni$	v	$::=$	ϕ, ψ, π
Expressions	$\ni$	e	$::=$	$e(v) \mid \textbf{if}(v)\ e$

$$e(\psi) \Downarrow \phi \tag{1.3}$$

Definition (Independency)

$$\forall \langle \psi_i, \psi_j \rangle \mid \psi_i \neq \psi_j \ : \\ e[\psi \mapsto \psi_i] \Downarrow \phi_i \ \wedge \ e[\psi \mapsto \psi_j] \Downarrow \phi_j \ \wedge \ \phi_i = \phi_j \\ \Rightarrow \ \phi \not\rightsquigarrow \psi \tag{1.4}$$

Notizen

Definitions
Recap
University of Freiburg

Definition (Direct Dependency [?, ?])

$e(\psi) \Downarrow \phi \ \Rightarrow \ \phi \rightsquigarrow \psi$

Definition (Indirect Dependency [?, ?])

$\textbf{if}\ (\psi)\ e \Downarrow \phi \ \Rightarrow \ \phi \rightsquigarrow \psi$

Definition (Transitiv Relation [?, ?])

$\phi \rightsquigarrow \pi \ \wedge \ \pi \rightsquigarrow \psi \ \Rightarrow \ \phi \rightsquigarrow \psi$

Notizen

Syntax of λ_{JS} [?]
University of Freiburg

$$
\begin{array}{llcl}
\textit{Constant} & \ni c & ::= & \textit{bool} \mid \textit{num} \mid \textit{str} \mid \textbf{undefined} \mid \textbf{null} \\
\textit{Variable} & \ni x & ::= & x_0 \ldots \\
\textit{Value} & \ni v & ::= & c \mid \xi^{\ell} \\
\textit{Expression} & \ni e & ::= & v \mid x \\
 & & \mid & \textbf{let}\ (x = e)\ \textbf{in}\ e \\
 & & \mid & \textbf{op}(e \ldots) \\
 & & \mid & e.e \\
 & & \mid & e.e = e \\
 & & \mid & e(e) \\
 & & \mid & \textbf{new}^{\ell} \\
 & & \mid & \textbf{if}\ (e)\ e,\ e \\
 & & \mid & \lambda^{\ell} x.e \\
 & & \mid & e; e \\
 & & \mid & \textbf{trace}^{\iota}(e)
\end{array}
$$

Notizen

Semantic domains

University of Freiburg

$$
\begin{array}{lllll}
Location & \ni & \xi^{\ell} & & \\
Function & \ni & \lambda^{\ell}x.e & & \\
Closure & \ni & f & ::= & Environment \times Function \\
Properties & \ni & \mathcal{P} & ::= & str \rightharpoonup Value \\
Object & \ni & o & ::= & Properties \times Closure \\
Environment & \ni & \rho & ::= & Variable \rightharpoonup Value \\
Heap & \ni & \mathcal{H} & ::= & Location \rightharpoonup Object
\end{array}
$$

Definition (Judgement λ_{JS})

$$\mathcal{H}, \rho \vdash e \Downarrow \mathcal{H}' \mid v \tag{2.1}$$

Notizen

Dependency Type

University of Freiburg

$$
\begin{array}{lllll}
Basic\ Value & \ni & v & ::= & c \\
 & & & \mid & \xi^{\ell} \\
Value & \ni & \omega & ::= & v : \kappa \\
Dependency\ Type & \ni & \kappa & ::= & \emptyset \\
 & & & \mid & \iota \\
 & & & \mid & \kappa \bullet \kappa
\end{array}
$$

Definition (Judgement $\lambda_{JS}^{\mathcal{D}}$)

$$\mathcal{H}, \rho, \kappa \vdash e \Downarrow \mathcal{H}' \mid \omega \tag{2.2}$$

Notizen

Evaluation of $\lambda_{JS}^{\mathcal{D}}$

Semantics

University of Freiburg

(DT-Constant)

$$\frac{}{\mathcal{H}, \rho, \kappa \vdash c \Downarrow \mathcal{H} \mid c : \kappa}$$

(DT-Variable)

$$\frac{}{\mathcal{H}, \rho, \kappa \vdash x \Downarrow \mathcal{H} \mid \rho(x) \bullet \kappa}$$

(DT-Operation)

$$\frac{\begin{array}{c}\mathcal{H}, \rho, \kappa \vdash e_0 \Downarrow \mathcal{H}' \mid v_0 : \kappa_0 \\ \vdots \\ \mathcal{H}^{n-1}, \rho, \kappa \vdash e_n \Downarrow \mathcal{H}^n \mid v_n : \kappa_n \\ v_{op} = \Downarrow_{\mathbf{op}}^{v} (v_0 \ldots v_n)\end{array}}{\mathcal{H}, \rho, \kappa \vdash \mathbf{op}(e_0 \ldots e_n) \Downarrow \mathcal{H}^n \mid v_{op} : \kappa_0 \bullet \ldots \bullet \kappa_n}$$

Notizen

(DT-Let)

$$\frac{\mathcal{H}, \rho, \kappa \vdash e_0 \Downarrow \mathcal{H}' \mid v_0 : \kappa_0 \qquad \mathcal{H}', \rho[x \mapsto v_0 : \kappa_0], \kappa \vdash e_1 \Downarrow \mathcal{H}'' \mid v_1 : \kappa_1}{\mathcal{H}, \rho, \kappa \vdash \textbf{let } (x = e_0) \textbf{ in } e_1 \Downarrow \mathcal{H}'' \mid v_1 : \kappa_1}$$

(DT-FunctionCreation)

$$\frac{\xi^{\ell} \notin dom(\mathcal{H})}{\mathcal{H}, \rho, \kappa \vdash \lambda^{\ell}x.e \Downarrow \mathcal{H}[\xi^{\ell} \mapsto \langle \rho, \lambda^{\ell}x.e \rangle] \mid \xi^{\ell} : \kappa}$$

(DT-FunctionApplication)

$$\frac{\mathcal{H}, \rho, \kappa \vdash e_0 \Downarrow \mathcal{H}' \mid \xi^{\ell} : \kappa_0 \qquad \langle \mathcal{P}, \langle \dot{\rho}, \lambda^{\ell}x.e \rangle \rangle = \mathcal{H}'(\xi^{\ell}) \qquad \mathcal{H}', \rho, \kappa \vdash e_1 \Downarrow \mathcal{H}'' \mid v_1 : \kappa_1 \qquad \mathcal{H}'', \dot{\rho}[x \mapsto v_1 : \kappa_1], \kappa \bullet \kappa_0 \vdash e \Downarrow \mathcal{H}''' \mid v : \kappa_v}{\mathcal{H}, \rho, \kappa \vdash e_0(e_1) \Downarrow \mathcal{H}''' \mid v : \kappa_v}$$

Notizen

(DT-ObjectCreation)

$$\frac{\xi^{\ell} \notin dom(\mathcal{H})}{\mathcal{H}, \rho, \kappa \vdash \textbf{new}^{\ell} \Downarrow \mathcal{H}[\xi^{\ell} \mapsto \emptyset] \mid \xi^{\ell} : \kappa}$$

(DT-PropertyReference)

$$\frac{\mathcal{H}, \rho, \kappa \vdash e_0 \Downarrow \mathcal{H}' \mid \xi^{\ell} : \kappa_{\xi^{\ell}} \qquad \mathcal{H}', \rho, \kappa \vdash e_1 \Downarrow \mathcal{H}'' \mid str : \kappa_{str}}{\mathcal{H}, \rho, \kappa \vdash e_0.e_1 \Downarrow \mathcal{H}'' \mid \mathcal{H}''(\xi^{\ell})(str) \bullet \kappa_{\xi^{\ell}} \bullet \kappa_{str}}$$

(DT-PropertyAssignment)

$$\frac{\mathcal{H}, \rho, \kappa \vdash e_0 \Downarrow \mathcal{H}' \mid \xi^{\ell} : \kappa_{\xi^{\ell}} \qquad \mathcal{H}', \rho, \kappa \vdash e_1 \Downarrow \mathcal{H}'' \mid str : \kappa_{str} \qquad \mathcal{H}'', \rho, \kappa \vdash e_2 \Downarrow \mathcal{H}''' \mid v : \kappa_v}{\mathcal{H}, \rho, \kappa \vdash e_0.e_1 = e_2 \Downarrow \mathcal{H}'''[\xi^{\ell}, str \mapsto v : \kappa_v \bullet \kappa_{\xi^{\ell}} \bullet \kappa_{str}] \mid v : \kappa_v}$$

Notizen

(DT-ConditionTrue)

$$\frac{\mathcal{H}, \rho, \kappa \vdash e_0 \Downarrow \mathcal{H}' \mid v_0 : \kappa_0 \qquad v_0 = true \qquad \mathcal{H}', \rho, \kappa \bullet \kappa_0 \vdash e_1 \Downarrow \mathcal{H}''_1 \mid v_1 : \kappa_1}{\mathcal{H}, \rho, \kappa \vdash \textbf{if } (e_0)\ e_1,\ e_2 \Downarrow \mathcal{H}''_1 \mid v_1 : \kappa_1}$$

(DT-ConditionFalse)

$$\frac{\mathcal{H}, \rho, \kappa \vdash e_0 \Downarrow \mathcal{H}' \mid v_0 : \kappa_0 \qquad v_0 \neq true \qquad \mathcal{H}', \rho, \kappa \bullet \kappa_0 \vdash e_2 \Downarrow \mathcal{H}''_2 \mid v_2 : \kappa_2}{\mathcal{H}, \rho, \kappa \vdash \textbf{if } (e_0)\ e_1,\ e_2 \Downarrow \mathcal{H}''_2 \mid v_2 : \kappa_2}$$

Notizen

Evaluation of $\lambda_{JS}^{\mathcal{D}}$

Semantics

University of Freiburg

(DT-Sequence)
$$\frac{\mathcal{H}, \rho, \kappa \vdash e_0 \Downarrow \mathcal{H}' \mid v_0 : \kappa_0 \qquad \mathcal{H}', \rho, \kappa \vdash e_1 \Downarrow \mathcal{H}'' \mid v_1 : \kappa_1}{\mathcal{H}, \rho, \kappa \vdash e_0; e_1 \Downarrow \mathcal{H}'' \mid v_1 : \kappa_1}$$

(DT-Trace)
$$\frac{\mathcal{H}, \rho, \kappa \bullet \iota \vdash e \Downarrow \mathcal{H}' \mid v : \kappa_v}{\mathcal{H}, \rho, \kappa \vdash \mathbf{trace}^{\iota}\ (e) \Downarrow \mathcal{H}' \mid v : \kappa_v}$$

Notizen

Lattice Value

University of Freiburg

Undefined	$::=$	$\{\texttt{undefined}, \bot\}$
Null	$::=$	$\{\texttt{null}, \bot\}$
Bool	$::=$	$\{\texttt{true}, \texttt{false}, \bot\}$
Infinity	$::=$	$\{+\texttt{Infinity}, -\texttt{Infinity}\}$
UInt	$::=$	$\{0 \ldots 4294967295\}$
NotUInt	$::=$	$\{\ldots, -1, -1.1, 1.1, \ldots\}$
Num	$::=$	*Infinity* $\cup$ *UInt* $\cup$ *NotUInt* $\cup$ $\{\texttt{NaN}, \bot\}$
UIntString	$::=$	$\{''0'' \ldots ''4294967295''\}$
NotUIntString	$::=$	$\{''a'', ''b'', \ldots\}$
String	$::=$	*UIntString* $\cup$ *NotUIntString* $\cup$ $\{\bot\}$

Lattice Value $\ni \mathcal{L}$ $::=$ *Undefined* $\times$ *Null* $\times$ *Bool* $\times$ *Num* $\times$ *String*

Notizen

Abstract Semantic Domains

University of Freiburg

SourceLocation	$\ni \ell, \iota$	$::=$	*sourcefile* $\times$ *linenumber*
Label	$\ni \Xi$	$::=$	$\{$*SourceLocation* $\ldots\}$
Abstract Closure	$\ni \Lambda^{\ell}$	$::=$	*Scope* $\times$ *Function*
PropertyMap	$\ni \Delta$	$::=$	*Lattice Value* $\rightarrow$ *Abstract Value*
Abstract Value	$\ni \vartheta$	$::=$	*Lattice Value* $\times$ *Label* $\times$ *Dependency*
Abstract Object	$\ni \theta$	$::=$	*PropertyMap* $\times$ *Abstract Closure*
FunctionStore	$\ni \mathcal{F}$	$::=$	*State* $\times$ *Abstract Value* $\times$ *State* $\times$ *Abstract Value*
Scope	$\ni \sigma$	$::=$	*Variable* $\rightarrow$ *Abstract Value*
State	$\ni \Gamma$	$::=$	(*SourceLocation* $\rightarrow$ *Abstract Object*) $\times$ *Dependency*

Notizen

Dependency $\mathcal{D}$

University of Freiburg

$$
\begin{array}{llll}
\textit{Trace} & \ni \tau & ::= & \textit{SourceLocation} \to \wp(\textit{Abstract Value}) \\
\textit{Dependency} & \ni \mathcal{D} & ::= & \emptyset \\
 & & \mid & \tau \\
 & & \mid & \mathcal{D}_0 \sqcup \mathcal{D}_1
\end{array}
$$

$$\circledcirc(\iota) = \tau_\iota \tag{3.1}$$

$$\circledcirc(\iota, \vartheta) \equiv \langle \mathcal{V}(\vartheta), \mathcal{D}_\vartheta \sqcup \tau_\iota \rangle \tag{3.2}$$

Notizen

Judgement

University of Freiburg

$$\Gamma, \sigma \vdash e \Downarrow \Gamma' \mid \vartheta \tag{3.3}$$

Notizen

Evaluation

Abstract Semantics

University of Freiburg

(A-Constant)
$$\frac{}{\Gamma, \sigma \vdash c \Downarrow \Gamma \mid \langle c, \emptyset, \mathcal{D}_\Gamma \rangle}$$

(A-Variable)
$$\frac{}{\Gamma, \sigma \vdash x \Downarrow \Gamma \mid \sigma(x) \sqcup \mathcal{D}_\Gamma}$$

(A-Let)
$$\frac{\Gamma, \sigma \vdash e_0 \Downarrow \Gamma' \mid \vartheta_0 \qquad \Gamma', \sigma[x \mapsto \vartheta_0] \vdash e_1 \Downarrow \Gamma'' \mid \vartheta_1}{\Gamma, \sigma \vdash \textbf{let } (x = e_0) \textbf{ in } e_1 \Downarrow \Gamma'' \mid \vartheta_1}$$

Notizen

(A-Operation)

$$\frac{\begin{array}{c}\Gamma,\sigma \ \vdash \ e_0 \ \Downarrow \ \Gamma' \mid \vartheta_0 \\ \vdots \\ \Gamma^{n-1},\sigma \ \vdash \ e_n \ \Downarrow \ \Gamma^n \mid \vartheta_n \\ \langle\mathcal{L},\Xi\rangle = \Downarrow^{\vartheta}_{\mathbf{op}} (\mathcal{V}(\vartheta_0)\ldots\mathcal{V}(\vartheta_n))\end{array}}{\Gamma,\sigma \ \vdash \ \mathbf{op}(e_0\ldots e_n) \ \Downarrow \ \Gamma^n \mid \langle\mathcal{L},\Xi,\mathcal{D}_{\vartheta_0}\sqcup\cdots\sqcup\mathcal{D}_{\vartheta_n}\rangle}$$

Notizen

(A-ObjectCreation1)

$$\frac{\ell \notin dom(\Gamma)}{\Gamma,\sigma \ \vdash \ \mathbf{new}^{\ell} \ \Downarrow \ \Gamma[\ell \mapsto \emptyset] \mid \langle\mathcal{L}_{\perp},\{\ell\},\mathcal{D}_{\Gamma}\rangle}$$

(A-ObjectCreation2)

$$\frac{\ell \in dom(\Gamma)}{\Gamma,\sigma \ \vdash \ \mathbf{new}^{\ell} \ \Downarrow \ \Gamma \mid \langle\mathcal{L}_{\perp},\{\ell\},\mathcal{D}_{\Gamma}\rangle}$$

Notizen

(A-FunctionCreation1)

$$\frac{\ell \notin dom(\Gamma) \qquad \mathcal{F}[\ell \mapsto \langle\Gamma_{\perp},\vartheta_{\perp},\Gamma_{\perp},\vartheta_{\perp}\rangle]}{\Gamma,\sigma \ \vdash \ \lambda^{\ell}x.e \ \Downarrow \ \Gamma[\ell \mapsto \langle\sigma,\lambda^{\ell}x.e\rangle] \mid \langle\mathcal{L}_{\perp},\{\ell\},\mathcal{D}_{\Gamma}\rangle}$$

(A-FunctionCreation2)

$$\frac{\ell \in dom(\Gamma) \qquad \langle\dot{\sigma},\lambda^{\ell}x.e\rangle = \Gamma(\ell)_{\Lambda^{\ell}}}{\Gamma,\sigma \ \vdash \ \lambda^{\ell}x.e \ \Downarrow \ \Gamma[\ell \mapsto \langle\sigma\sqcup\dot{\sigma},\lambda^{\ell}x.e\rangle] \mid \langle\mathcal{L}_{\perp},\{\ell\},\mathcal{D}_{\Gamma}\rangle}$$

Notizen

(A-FunctionApplication)

$$\frac{\Gamma, \sigma \vdash e_0 \Downarrow \Gamma' \mid \langle \mathcal{L}_0, \Xi_0, \mathcal{D}_0 \rangle \qquad \Gamma', \sigma \vdash e_1 \Downarrow \Gamma'' \mid \vartheta_1 \qquad \Gamma''[\mathcal{D} \mapsto \mathcal{D}_{\Gamma''} \sqcup \mathcal{D}_0] \vdash^{\Pi}_{\mathbf{FA}} \Gamma'(\Xi_0), \vartheta_1 \Downarrow \Gamma''' \mid \vartheta}{\Gamma, \sigma \vdash e_0(e_1) \Downarrow \langle \mathcal{S}(\Gamma'''), \mathcal{D}_\Gamma \rangle \mid \vartheta}$$

(FA-Iteration1)

$$\frac{\Gamma \vdash^{\Lambda^\ell}_{\mathbf{FA}} \Lambda^\ell, \vartheta \Downarrow \Gamma' \mid \vartheta' \qquad \Gamma' \vdash^{\Pi}_{\mathbf{FA}} \Pi, \vartheta \Downarrow \Gamma'' \mid \vartheta''}{\Gamma \vdash^{\Pi}_{\mathbf{FA}} \Lambda^\ell; \Pi, \vartheta \Downarrow \Gamma'' \mid \vartheta' \sqcup \vartheta''}$$

(FA-Iteration2)

$$\frac{}{\Gamma \vdash^{\Pi}_{\mathbf{FA}} \emptyset, \vartheta \Downarrow \Gamma \mid \vartheta_\perp}$$

Notizen

(FA-FunctionStore1)

$$\frac{\langle \Gamma, \vartheta \rangle \sqsubseteq \mathcal{F}(\Lambda^\ell)_{\Lambda^\ell_{In}} \qquad \langle \Gamma', \vartheta' \rangle = \mathcal{F}(\ell)_{\Lambda^\ell_{Out}}}{\Gamma \vdash^{\Lambda^\ell}_{\mathbf{FA}} \Lambda^\ell, \vartheta \Downarrow \Gamma' \mid \vartheta'}$$

(FA-FunctionStore2)

$$\frac{\begin{matrix} \langle \Gamma, \vartheta \rangle \not\sqsubseteq \mathcal{F}(\Lambda^\ell)_{\Lambda^\ell_{In}} & \langle \dot{\sigma}, \lambda^\ell x.e \rangle = \theta_{\Lambda^\ell} \\ \langle \bar{\Gamma}, \bar{\vartheta} \rangle = \mathcal{F}(\ell)_{\Lambda^\ell_{In}} \sqcup \langle \Gamma, \vartheta \rangle & \mathcal{F}[\ell, \Lambda^\ell_{In} \mapsto \langle \bar{\Gamma}, \bar{\vartheta} \rangle] \\ \bar{\Gamma}, \dot{\sigma}[x \mapsto \bar{\vartheta}] \vdash e \Downarrow \bar{\Gamma}' \mid \bar{\vartheta}' & \mathcal{F}[\ell, \Lambda^\ell_{Out} \mapsto \langle \bar{\Gamma}', \bar{\vartheta}' \rangle] \end{matrix}}{\Gamma \vdash^{\Lambda^\ell}_{\mathbf{FA}} \Lambda^\ell, \vartheta \Downarrow \bar{\Gamma}' \mid \bar{\vartheta}'}$$

Notizen

(A-PropertyReference)

$$\frac{\Gamma, \sigma \vdash e_0 \Downarrow \Gamma' \mid \langle \mathcal{L}_0, \Xi_0, \mathcal{D}_0 \rangle \qquad \Gamma', \sigma \vdash e_1 \Downarrow \Gamma'' \mid \langle \mathtt{str}, \Xi_1, \mathcal{D}_1 \rangle \qquad \vdash^{\Theta}_{\mathbf{PR}} \Gamma''(\Xi_0), \mathtt{str} \Downarrow \vartheta}{\Gamma, \sigma \vdash e_0.e_1 \Downarrow \Gamma'' \mid \langle \mathcal{V}(\vartheta), \mathcal{D}_0 \sqcup \mathcal{D}_1 \sqcup \mathcal{D}_\vartheta \rangle}$$

(PR-Iteration1)

$$\frac{\vdash^{\Delta}_{\mathbf{PR}} \Delta, \mathcal{L} \Downarrow \vartheta \qquad \vdash^{\Theta}_{\mathbf{PR}} \Theta, \mathcal{L} \Downarrow \vartheta'}{\vdash^{\Theta}_{\mathbf{PR}} \langle \Delta, \Lambda^\ell \rangle : \Theta, \mathcal{L} \Downarrow \vartheta \sqcup \vartheta'}$$

(PR-Iteration2)

$$\frac{}{\vdash^{\Theta}_{\mathbf{PR}} \emptyset, \mathcal{L} \Downarrow \vartheta_\perp}$$

Notizen

(PR-Intersection)

$$\frac{\begin{array}{c}(\mathcal{L} \sqcap \mathcal{L}_i \neq \bot) \\ \vdash^{\ominus}_{\mathbf{PR}} \;\Delta, \mathcal{L} \;\Downarrow\; \vartheta'\end{array}}{\vdash^{\Delta}_{\mathbf{PR}} \;(\mathcal{L}_i : \vartheta_i); \Delta, \mathcal{L} \;\Downarrow\; \vartheta_i \sqcup \vartheta'}$$

(PR-NonIntersection)

$$\frac{\begin{array}{c}\mathcal{L} \sqcap \mathcal{L}_i = \bot \\ \vdash^{\ominus}_{\mathbf{PR}} \;\Delta, \mathcal{L} \;\Downarrow\; \vartheta'\end{array}}{\vdash^{\Delta}_{\mathbf{PR}} \;(\mathcal{L}_i : \vartheta_i); \Delta, \mathcal{L} \;\Downarrow\; \vartheta'}$$

(PR-Empty)

$$\frac{}{\vdash^{\Delta}_{\mathbf{PR}} \;\emptyset, \mathcal{L} \;\Downarrow\; \vartheta_{undef}}$$

Notizen

(A-PopertyAssignment)

$$\frac{\begin{array}{c}\Gamma, \sigma \;\vdash\; e_0 \;\Downarrow\; \Gamma' \mid \langle \mathcal{L}_0, \Xi_0, \mathcal{D}_0 \rangle \\ \Gamma', \sigma \;\vdash\; e_1 \;\Downarrow\; \Gamma'' \mid \langle \mathtt{str}, \Xi_1, \mathcal{D}_1 \rangle \\ \Gamma'', \sigma \;\vdash\; e_2 \;\Downarrow\; \Gamma''' \mid \vartheta \\ \Gamma''' \;\vdash^{\Xi}_{\mathbf{PA}} \;\Xi_0, \mathtt{str}, \langle \mathcal{V}(\vartheta), \mathcal{D}_0 \sqcup \mathcal{D}_1 \sqcup \mathcal{D}_\vartheta \rangle \;\Downarrow\; \Gamma''''\end{array}}{\Gamma, \sigma \;\vdash\; e_0.e_1 = e_2 \;\Downarrow\; \Gamma'''' \mid \vartheta}$$

(PA-Iteration1)

$$\frac{\begin{array}{c}\Gamma \;\vdash^{\ell}_{\mathbf{PA}} \;\ell, \mathcal{L}, \vartheta \;\Downarrow\; \Gamma' \\ \Gamma' \;\vdash^{\Xi}_{\mathbf{PA}} \;\Xi, \mathcal{L}, \vartheta \;\Downarrow\; \Gamma''\end{array}}{\Gamma \;\vdash^{\Xi}_{\mathbf{PA}} \;\ell; \Xi, \mathcal{L}, \vartheta \;\Downarrow\; \Gamma''}$$

(PA-Iteration2)

$$\frac{}{\Gamma \;\vdash^{\Xi}_{\mathbf{PA}} \;\emptyset, \mathcal{L}, \vartheta \;\Downarrow\; \Gamma}$$

Notizen

(PA-Assignment1)

$$\frac{\mathcal{L} \in dom(\Gamma(l))}{\Gamma \;\vdash^{\ell}_{\mathbf{PA}} \;\ell, \mathcal{L}, \vartheta \;\Downarrow\; \Gamma[\ell, \mathcal{L} \mapsto \Gamma(\ell)(\mathcal{L}) \sqcup \vartheta]}$$

(PA-Assignment2)

$$\frac{\mathcal{L} \notin dom(\Gamma(\ell))}{\Gamma \;\vdash^{\ell}_{\mathbf{PA}} \;\ell, \mathcal{L}, \vartheta \;\Downarrow\; \Gamma[\ell, \mathcal{L} \mapsto \vartheta]}$$

Notizen

(A-ConditionTrue)

$$\frac{\Gamma, \sigma \vdash e_0 \Downarrow \Gamma' \mid \langle \mathcal{L}_0, \Xi_0, \mathcal{D}_0 \rangle \quad \mathcal{L}_0 = \texttt{true} \quad \Gamma'[\mathcal{D} \mapsto \mathcal{D}_{\Gamma'} \sqcup \mathcal{D}_0], \sigma \vdash e_1 \Downarrow \Gamma'' \mid \vartheta_1}{\Gamma, \sigma \vdash \textbf{if}\ (e_0)\ e_1,\ e_2 \Downarrow \langle \mathcal{S}(\Gamma''), \mathcal{D}_\Gamma \rangle \mid \vartheta_1}$$

(A-ConditionFalse)

$$\frac{\Gamma, \sigma \vdash e_0 \Downarrow \Gamma' \mid \langle \mathcal{L}_0, \Xi_0, \mathcal{D}_0 \rangle \quad \mathcal{L}_0 = \texttt{false} \quad \Gamma'[\mathcal{D} \mapsto \mathcal{D}_{\Gamma'} \sqcup \mathcal{D}_0], \sigma \vdash e_2 \Downarrow \Gamma'' \mid \vartheta_2}{\Gamma, \sigma \vdash \textbf{if}\ (e_0)\ e_1,\ e_2 \Downarrow \langle \mathcal{S}(\Gamma''), \mathcal{D}_\Gamma \rangle \mid \vartheta_2}$$

Notizen

(A-Condition)

$$\frac{\begin{array}{c}\Gamma, \sigma \vdash e_0 \Downarrow \Gamma' \mid \langle \mathcal{L}_0, \Xi_0, \mathcal{D}_0 \rangle \\ \mathcal{L}_0 \neq \texttt{true} \wedge \mathcal{L}_0 \neq \texttt{false} \\ \Gamma'[\mathcal{D} \mapsto \mathcal{D}_{\Gamma'} \sqcup \mathcal{D}_0], \sigma \vdash e_1 \Downarrow \Gamma_1'' \mid \vartheta_1 \\ \Gamma'[\mathcal{D} \mapsto \mathcal{D}_{\Gamma'} \sqcup \mathcal{D}_0], \sigma \vdash e_2 \Downarrow \Gamma_2'' \mid \vartheta_2\end{array}}{\Gamma, \sigma \vdash \textbf{if}\ (e_0)\ e_1,\ e_2 \Downarrow \langle \mathcal{S}(\Gamma_1'' \sqcup \Gamma_2''), \mathcal{D}_\Gamma \rangle \mid \vartheta_1 \sqcup \vartheta_2}$$

Notizen

(A-Sequence)

$$\frac{\begin{array}{c}\Gamma, \sigma \vdash e_0 \Downarrow \Gamma' \mid \vartheta_0 \\ \Gamma', \sigma \vdash e_1 \Downarrow \Gamma'' \mid \vartheta_1\end{array}}{\Gamma, \sigma \vdash e_0; e_1 \Downarrow \Gamma'' \mid \vartheta_1}$$

(A-Trace)

$$\frac{\begin{array}{c}\tau_\iota = \circledcirc(\iota) \\ \Gamma[\mathcal{D} \mapsto \mathcal{D}_\Gamma \sqcup \tau_\iota], \sigma \vdash e \Downarrow \Gamma' \mid \vartheta\end{array}}{\Gamma, \sigma \vdash \textbf{trace}^\iota\ (e) \Downarrow \langle \mathcal{S}(\Gamma'), \mathcal{D}_\Gamma \rangle \mid \vartheta}$$

Notizen

Soundness

University of Freiburg

1. Noninterference on $\lambda_{JS}^{\mathcal{D}}$
2. Correctness ($\mathcal{C}$-Consistency)
3. Termination

Notizen

Noninterference

University of Freiburg

$$\mathcal{H}, \rho, \kappa \vdash e \Downarrow \mathcal{H}' \mid v : \kappa_v \tag{4.1}$$

$$\iota \notin \kappa_v : \mathcal{H}, \rho, \kappa \vdash \bar{e} \Downarrow \tilde{\mathcal{H}}' \mid v : \kappa_v \tag{4.2}$$

$$\bar{e} = e[\iota \mapsto \tilde{e}] \tag{4.3}$$

Notizen

Substitution of ι

University of Freiburg

Definition (Substitution of ι)

The substitution $e[\iota \mapsto \tilde{e}]$ of ι in e is defined as:

$$\forall e' \in SubExp(e) : \; e'[\iota \mapsto \tilde{e}] \tag{4.4}$$

$$\mathbf{trace}^{\iota}(e_{\iota})[\iota \mapsto \tilde{e}] \equiv \mathbf{trace}^{\iota}(\tilde{e}) \tag{4.5}$$

Termination-Insensitive Noninterference

Notizen

Bijection of ξ^ℓ

University of Freiburg

UNI FREIBURG

Definition (Bijection of ξ^ℓ)

The bijection $\flat$: *Location* $\rightarrow$ *Location* from location ξ^ℓ to location $\xi^{\ell\prime}$ maps permutations on heap entries.

$$\flat \ ::= \ \emptyset \mid \flat[\xi^\ell \mapsto \xi^{\ell\prime}] \tag{4.6}$$

Definition (Bijection of v)

The bijection $\flat$ for values is defined as:

$$\flat(v) \ ::= \ \begin{cases} \flat(\xi^\ell) & v = \xi^\ell \\ v & v \neq \xi^\ell \end{cases} \tag{4.7}$$

Notizen

κ-equivalence of $\mathcal{H}$

University of Freiburg

UNI FREIBURG

Definition (κ-equivalence)

Two heaps $\mathcal{H}_0$,$\mathcal{H}_1$ are κ-equivalent $\mathcal{H}_0 \equiv_{\flat,\kappa} \mathcal{H}_1$ iff

$$\forall \xi^\ell \in dom(\flat) : \ \mathcal{H}_0(\xi^\ell) \equiv_{\flat,\kappa} \mathcal{H}_1(\flat(\xi^\ell)) \tag{4.8}$$

The heaps $\mathcal{H}_0$,$\mathcal{H}_1$ only differ in values $v : \kappa_v$ with any intersection with κ or in one-sided locations.

Notizen

κ-equivalence of o

University of Freiburg

UNI FREIBURG

Definition (κ-equivalence)

Two objects o_0,o_1 are κ-equivalent $\langle \mathcal{P}_0, \langle \rho_0, \lambda^\ell x.e_0 \rangle\rangle \equiv_{\flat,\kappa} \langle \mathcal{P}_1, \langle \rho_1, \lambda^\ell x.e_1 \rangle\rangle$ iff

$$\begin{aligned} &\forall str \in dom(\mathcal{P}_0) : \\ &str \in dom(\mathcal{P}_1) \ \wedge \ \mathcal{P}_0(str) = \mathcal{P}_1(str) \ \vee && (4.9) \\ &\mathcal{P}_0(str) = v : \kappa_v \ \wedge \ \kappa \cap \kappa_v \neq \emptyset \\ &\forall str \in dom(\mathcal{P}_1) : \\ &str \in dom(\mathcal{P}) \ \wedge \ \mathcal{P}_0(str) = \mathcal{P}_1(str) \ \vee && (4.10) \\ &\mathcal{P}_1(str) = v : \kappa_v \ \wedge \ \kappa \cap \kappa_v \neq \emptyset \\ &\rho_0 \equiv_{\flat,\kappa} \rho_1 \ \wedge \ \lambda^\ell x.e_0 \equiv_{\flat,\kappa} \lambda^\ell x.e_1 && (4.11) \end{aligned}$$

The objects o_0,o_1 only differ in values $v : \kappa_v$ with any intersection with κ.

Notizen

κ-equivalence of ρ

University of Freiburg

UNI FREIBURG

Definition (κ-equivalence)

Two environments ρ_0,ρ_1 are κ-equivalent $\rho_0 \equiv_{\flat,\kappa} \rho_1$ iff

$$\begin{aligned} &\forall x \in dom(\rho_0): \\ &x \in dom(\rho_1) \;\wedge\; \rho_0(x) = \rho_1(x) \;\vee \qquad (4.12) \\ &\rho_0(x) = v : \kappa_v \;\wedge\; \kappa \cap \kappa_v \neq \emptyset \\ &\forall x \in dom(\rho_1): \\ &x \in dom(\rho_0) \;\wedge\; \rho_0(x) = \rho_1(x) \;\vee \qquad (4.13) \\ &\rho_1(x) = v : \kappa_v \;\wedge\; \kappa \cap \kappa_v \neq \emptyset \end{aligned}$$

The environments ρ_0,ρ_1 only differ in values $v : \kappa_v$ with any intersection with κ.

Notizen

κ-equivalence of ω

University of Freiburg

UNI FREIBURG

Definition (κ-equivalence)

Two value ω_0,ω_1 are κ-equivalent $v_0 : \kappa_0 \equiv_{\flat,\kappa} v_1 : \kappa_1$ iff

$$\kappa \cap \kappa_0 = \emptyset \;\wedge\; \kappa \cap \kappa_1 = \emptyset \;\rightarrow\; \flat(v_0) = v_1 \qquad (4.14)$$

The values ω_0,ω_1 only differ in the case of any intersection with κ.

Notizen

κ-equivalence of e

University of Freiburg

UNI FREIBURG

Definition (κ-equivalence)

Two expressions e_0,e_1 are κ-equivalent $e_0 \equiv_{\flat,\kappa} e_1$ iff

$$\kappa = \{\iota_0, ..., \iota_n\} \;\rightarrow\; \exists e_0' \dots \exists e_n' : \; e_0 \;=\; e_1[\iota_0 \mapsto e_0'] \dots [\iota_n \mapsto e_n'] \qquad (4.15)$$

The expressions e_0,e_1 only differ below $\textbf{trace}^{\iota}(e_\iota)$ subexpressions with $\iota \in \kappa$.

Notizen

Context Dependency

Theorem

University of Freiburg

Theorem (Context Dependency)

We assume that $\forall \mathcal{H}, \rho, \kappa, e:\ \mathcal{H}, \rho, \kappa \ \vdash\ e \Downarrow \mathcal{H}' \mid v : \kappa_v$ *implies that* $\kappa \subseteq \kappa_v$.

Notizen

Noninterference

Theorem

University of Freiburg

Theorem (Noninterference)

We assume $\forall \bar{\kappa}, \forall \flat$ *that*
$\forall \mathcal{H}, \tilde{\mathcal{H}}, \rho, \tilde{\rho}, \kappa, e:\ \mathcal{H}, \rho, \kappa \ \vdash\ e \Downarrow \mathcal{H}' \mid v : \kappa_v$.
If $\iota \notin \bar{\kappa}$ *and* $\mathcal{H} \equiv_{\flat,\{\iota \mid \iota \notin \bar{\kappa}\}} \tilde{\mathcal{H}}$ *and* $\rho \equiv_{\flat,\{\iota \mid \iota \notin \bar{\kappa}\}} \tilde{\rho}$ *then*
$\tilde{\mathcal{H}}, \tilde{\rho}, \kappa \ \vdash\ \bar{e} \Downarrow \tilde{\mathcal{H}}' \mid \tilde{v} : \tilde{\kappa}_v$ *with* $\bar{e} = e[\iota \mapsto \tilde{e}]$ *and* $e \equiv_{\flat,\{\iota \mid \iota \notin \bar{\kappa}\}} \bar{e}$
and $\mathcal{H}' \equiv_{\flat,\{\iota \mid \iota \notin \bar{\kappa}\}} \tilde{\mathcal{H}}'$ *and* $v : \kappa_v \equiv_{\flat,\{\iota \mid \iota \notin \bar{\kappa}\}} \tilde{v} : \tilde{\kappa}_v$.

Notizen

Correctness

University of Freiburg

$\forall e$:

$$\mathcal{H}, \rho, \kappa \ \vdash\ e \Downarrow \mathcal{H}' \mid \omega \tag{4.16}$$
$$\Gamma, \sigma \ \vdash\ e \Downarrow \Gamma' \mid \vartheta \tag{4.17}$$

$$\begin{aligned} &\mathcal{H} \prec_C \Gamma \ \wedge\ \rho \prec_C \sigma \ \wedge\ \kappa \prec_C \mathcal{D}_\Gamma \ \rightarrow \\ &\mathcal{H}' \prec_C \Gamma' \ \wedge\ \omega \prec_C \vartheta \end{aligned} \tag{4.18}$$

Notizen

$\mathcal{C}$-Consistency

University of Freiburg

Definition ($\mathcal{C}$-Consistency on dependencies $\kappa \prec_{\mathcal{C}} \mathcal{D}$)

$$\forall \iota \in \kappa : \; \tau_\iota \in \mathcal{D} \tag{4.19}$$

Definition ($\mathcal{C}$-Consistency on constants $c \prec_{\mathcal{C}} \mathcal{L}$)

$$c \in \mathcal{L} \tag{4.20}$$

Notizen

$\mathcal{C}$-Consistency

University of Freiburg

Definition ($\mathcal{C}$-Consistency on location $\xi^\ell \prec_{\mathcal{C}} \Xi$)

$$\ell \in \Xi \tag{4.21}$$

Definition ($\mathcal{C}$-Consistency on values $\omega \prec_{\mathcal{C}} \vartheta$)

$$\kappa \prec_{\mathcal{C}} D \tag{4.22}$$

$$v \in \mathcal{V}(\vartheta) \; ::= \begin{cases} \ell \in \Xi, & v = \xi^\ell \\ c \in \mathcal{L}, & v = c \end{cases} \tag{4.23}$$

Notizen

$\mathcal{C}$-Consistency

University of Freiburg

Definition ($\mathcal{C}$-Consistency on properties $\mathcal{P} \prec_{\mathcal{C}} \Delta$)

$$\forall str \in dom(\mathcal{P}) : \; \exists \mathcal{L} \in dom(\Delta) : \; str \in \mathcal{L} \; \wedge \; \mathcal{P}(str) \prec_{\mathcal{C}} \Delta(\mathcal{L}) \tag{4.24}$$

$$\forall str \notin dom(\mathcal{P}) : \; \textbf{undefined} \prec_{\mathcal{C}} \Delta(str) \tag{4.25}$$

Definition ($\mathcal{C}$-Consistency on objects $o \prec_{\mathcal{C}} \theta$)

$$\mathcal{P} \prec_{\mathcal{C}} \Delta \tag{4.26}$$

$$\rho \prec_{\mathcal{C}} \sigma \tag{4.27}$$

Notizen

$\mathcal{C}$-Consistency

University of Freiburg

Definition ($\mathcal{C}$-Consistency on scopes $\rho \prec_{\mathcal{C}} \sigma$)

$$\forall x \in dom(\rho): \; x \in dom(\sigma) \;\wedge\; \rho(x) \prec_{\mathcal{C}} \sigma(x) \tag{4.28}$$

Definition ($\mathcal{C}$-Consistency on heaps $\mathcal{H} \prec_{\mathcal{C}} \Gamma$)

$$\forall \xi^{\ell} \in dom(\mathcal{H}): \; \ell \in \Sigma \;\wedge\; \mathcal{H}(\xi^{\ell}) \prec_{\mathcal{C}} \Sigma(\ell) \tag{4.29}$$

Notizen

$\mathcal{C}$-Consistency

University of Freiburg

Lemma (Subset $\mathcal{C}$-Consistency)

$$\mathcal{H} \prec_{\mathcal{C}} \Gamma_0 \;\wedge\; \Gamma_0 \sqsubseteq \Gamma_1 \;\rightarrow\; \mathcal{H} \prec_{\mathcal{C}} \Gamma_1 \tag{4.30}$$

$$v : \kappa \prec_{\mathcal{C}} \vartheta_0 \;\wedge\; \vartheta_0 \sqsubseteq \vartheta_1 \;\rightarrow\; v : \kappa \prec_{\mathcal{C}} \vartheta_1 \tag{4.31}$$

Lemma ($\mathcal{C}$-Consistency on Property Update)

$$\forall o, \theta, \mathcal{L}, \vartheta \mid o \prec_{\mathcal{C}} \theta \;:\; o \prec_{\mathcal{C}} \theta[\mathcal{L} \mapsto \theta(\mathcal{L}) \sqcup \vartheta] \tag{4.32}$$

Notizen

Correctness

Theorem

University of Freiburg

Theorem (Correctness Relation)

For all expressions e within the syntax of $\lambda_{JS}^{\mathcal{D}}$ the following condition holds: $\forall \mathcal{H}, \mathcal{H}', \rho, v, \kappa$: If $\mathcal{H}, \rho, \kappa \vdash e \Downarrow \mathcal{H}' \mid v$ than $\forall \Gamma, \sigma$ with $\mathcal{H} \prec_{\mathcal{C}} \Gamma$, $\rho \prec_{\mathcal{C}} \sigma$ and $\kappa \prec_{\mathcal{C}} \mathcal{D}_{\Gamma}$: $\Gamma, \sigma \vdash e \Downarrow \Gamma' \mid \vartheta$ with $\mathcal{H}' \prec_{\mathcal{C}} \Gamma'$ and $v \prec_{\mathcal{C}} \vartheta$.

Notizen

Termination
Theorem
University of Freiburg

Theorem (Termination)

$\Gamma, \sigma \vdash e \Downarrow \Gamma' \mid \vartheta$ *with arbitrary e.*

1. Monotony
2. Ascending chain condition

Notizen

Access Permission Contracts [?]
Recap
University of Freiburg

```
function fun() {
  "Contract: a.b, a.b.c, a.?, a.b*.c"
  var x = a.b;
  a = {b:5};
}
```


Notizen

Dependency-based Access Permission Contracts
University of Freiburg

- Dependency-based
  - *TAJS*, static dependency analysis
- *Contracts* instead of **trace**$'(e)$
- $\mathcal{C}$: `Contract: a.b [r,w];`

Evaluation

1. *trace* values ϑ / state Γ
2. create proof constraints $\mathcal{L}$
3. validate constraints $\mathcal{L}$

Notizen

Constraint Based Proof constraints $\mathcal{L}$ at the end
Lazy Enforcement No direct enforcement of contracts $\mathcal{C}$
Dynamic Extent Nested contracts $\mathcal{C}$
Pre-State Snapshot $\Gamma, \sigma, \vartheta$ at $\mathcal{C}$
Read-Write Protection $\Gamma, \sigma, \vartheta$ at $\mathcal{C}$

Notizen

$$
\begin{array}{llcl}
\textit{Contract} & \ni \mathcal{C} & ::= & \emptyset \mid \mathcal{Q};\mathcal{C} \\
\textit{Permissions} & \ni \mathcal{Q} & ::= & \langle \mathcal{A}, \Pi \rangle \\
\\
\textit{AccessPath} & \ni \mathcal{A} & ::= & \vec{v}.\mathcal{P} \\
\textit{Properties} & \ni \mathcal{P} & ::= & \epsilon \mid \vec{p}.\mathcal{P} \mid \vec{p}*.\mathcal{P} \\
\textit{Variable} & \ni \vec{v} & ::= & \{x \ldots\} \\
\textit{Property} & \ni \vec{p} & ::= & \{x \ldots\} \\
\\
\textit{PathPermission} & \ni \Pi & ::= & \langle \pi_r, \pi_w \rangle \\
\textit{Readable} & \ni \pi_r & ::= & \epsilon \mid r \\
\textit{Writeable} & \ni \pi_w & ::= & \epsilon \mid w
\end{array}
$$

Notizen

$$
\begin{array}{ll}
\textit{ReadConstraint} & \ni \mathcal{R} \\
\textit{WriteConstraint} & \ni \mathcal{W}
\end{array}
$$

(DT-Permit)

$$
\frac{\begin{array}{c}\mathcal{H}, \rho, \kappa \vdash^{\mathcal{C}}_{\mathsf{Apply}} \mathcal{C}, \iota_{\mathcal{R}}, \iota_{\mathcal{W}} \Downarrow \mathcal{H}' \mid \rho' \mid \kappa' \mid \mathcal{L} \\ \mathcal{H}', \rho', \kappa' \vdash e \Downarrow \mathcal{H}'' \mid v : \kappa_v \\ \mathcal{H}'', \rho', \kappa_v \vdash^{\mathcal{C}}_{\mathsf{Check}} \mathcal{L}\end{array}}{\mathcal{H}, \rho, \kappa \vdash \textbf{permit}^{\iota_{\mathcal{R}}, \iota_{\mathcal{W}}}\ \mathcal{C}\ \textbf{in}\ e \Downarrow \mathcal{H}'' \mid v : \kappa_v}
$$

Notizen

UNI FREIBURG

Thank you for your attention.

Notizen

Notizen

Notizen