KTH ROYAL INSTITUTE
OF TECHNOLOGY

Degree Project in Technology

First cycle, 15 credits

# This is the title in the language of the thesis

A subtitle in the language of the thesis

**FAKE A. STUDENT**
**FAKE B. STUDENT**

Stockholm, Sweden, 2024

# This is the title in the language of the thesis

## A subtitle in the language of the thesis

FAKE A. STUDENT

FAKE B. STUDENT

Bachelor’s Programme in Information and Communication Technology
Date: February 5, 2024

Supervisors: A. Busy Supervisor, Another Busy Supervisor, Third Busy Supervisor
Examiner: Gerald Q. Maguire Jr.
School of Electrical Engineering and Computer Science
Host company: Företaget AB
Swedish title: Detta är den svenska översättningen av titeln
Swedish subtitle: Detta är den svenska översättningen av undertiteln

## 0.1 Inference Rules

### 0.1.1 Extension

#### 0.1.1.1 Typing

$$\text{T-ASYNC}\ \frac{\begin{array}{cc} Perm[Q] \in \Gamma & \Gamma \setminus Perm[Q]; a \vdash s : \sigma \\ \Gamma; a \vdash b : Q \rhd Box[C] & x : C; ocap \vdash t : \tau \end{array}}{\Gamma; a \vdash async(b)\{x \Rightarrow t\}\{s\} : \bot}$$

—

$$\text{T-FINISH}\ \frac{\Gamma; ocap \vdash t : \tau}{\Gamma; a \vdash finish\{t\} : null}$$

—

#### 0.1.1.2 Evaluation

$$\text{E-ASYNC}\ \frac{\begin{array}{cc} L(b) = b(o, p) & p \in P \\ T_1 = (f, \langle L,\ s,\ P \setminus \{p\}\rangle^{\epsilon}) & T_2 = (f, \langle [x \to o],\ t,\ \emptyset\rangle^{\epsilon}) \end{array}}{\begin{array}{l} H, \{(f, \langle L,\ async(b)\{x \Rightarrow t\}\{s\},\ P\rangle^{l} \circ FS)\} \uplus TS \\ \rightsquigarrow\ H, \{T_1, T_2\} \uplus TS \end{array}}$$

—

$$\text{E-FINISH1}\ \frac{T = (f', \langle L,\ t,\ P\rangle^{\epsilon}) \quad f' fresh}{\begin{array}{l} H, \{(f, \langle L,\ let\ x = finish\{\ t\ \}\ in\ s,\ P\rangle^{l} \circ FS)\} \uplus TS \\ \rightsquigarrow\ H, \{(f, \langle FINISH f'\rangle \circ \langle L[x \to null],\ s,\ P\rangle^{l} \circ FS)\} \uplus \{T\} \uplus TS \end{array}}$$

—

$$\text{E-FINISH2}\ \frac{\nexists (f', FS) \in TS}{\begin{array}{l} H, \{(f, \langle FINISH f'\rangle \circ FS)\} \uplus TS \\ \rightsquigarrow\ H, \{(f, FS)\} \uplus TS \end{array}}$$

—

$$\text{E-TASK-DONE}\ \frac{}{H, \{(f, \epsilon)\} \uplus TS \rightsquigarrow TS}$$

### 0.1.2 LaCasa

#### 0.1.2.1 Well-Formedness

$$\text{WF-VAR}\ \frac{\begin{array}{c} L(x) = null \vee \\ L(x) = o \wedge typeof(H, o) <: \Gamma(x) \vee \\ L(x) = b(o, p) \wedge \Gamma(x) = Q \rhd Box[C] \wedge typeof(H, o) <: C \end{array}}{H \vdash \Gamma; L; x}$$

—

$$\text{WF-PERM}\ \frac{\begin{array}{c}\gamma : permTypes(\Gamma) \longrightarrow Pinjective \\ \forall x \in dom(\Gamma). \\ (\Gamma(x) = Q \rhd Box[C] \wedge L(x) = b(o,p) \wedge Perm[Q] \in \Gamma) \\ \Longrightarrow \gamma(Q) = p\end{array}}{\vdash \Gamma; L; P}$$

—–

$$\text{WF-ENV}\ \frac{\begin{array}{c}dom(\Gamma) \subseteq dom(L) \\ \forall x \in dom(\Gamma). H \vdash \Gamma; L; x\end{array}}{H \vdash \Gamma; L}$$

—–

$$\text{WF-METHOD1}\ \frac{\Gamma_0, this : C, x : D; \epsilon \vdash t : E' \qquad E' <: E}{C \vdash defm(x : D) : E = t}$$

—–

$$\text{WF-METHOD2}\ \frac{\Gamma = \Gamma_0, this : C, x : Q \rhd Box[D], Perm[Q] \qquad Qfresh \qquad \Gamma; \epsilon \vdash t : E' \qquad E' <: E}{C \vdash defm(x : Box[D]) : E = t}$$

—–

$$\text{WF-PROGRAM}\ \frac{p \vdash \bar{cd} \qquad p \vdash \Gamma_0 \qquad \Gamma_0; \epsilon \vdash t : \sigma}{p \vdash \bar{cd}\bar{vd}t}$$

—–

$$\text{WF-CLASS}\ \frac{\begin{array}{c}C \vdash \bar{md} \qquad D = AnyRef \vee p \vdash classD... \\ \forall (defm...) \in \bar{md}.override(m, C, D) \\ \forall varf : \sigma \in \bar{fd}.f \notin fields(D)\end{array}}{p \vdash classCextendsD\{\bar{fd}\bar{md}\}}$$

—–

$$\text{WF-OVERRIDE}\ \frac{mtype(m, D)notdefined \vee mtype(m, D) = mtype(m, C)}{override(m, C, D)}$$

#### 0.1.2.2 Typing

$$\text{T-NULL}\ \frac{}{\Gamma; a \vdash null : Null}$$

—–

$$\text{T-VAR}\ \frac{x \in dom(\Gamma)}{\Gamma; a \vdash x : \Gamma(x)}$$

—–

$$\text{T-LET}\ \frac{\Gamma; a \vdash e : \tau \qquad \Gamma, x : \tau; a \vdash t : \sigma}{\Gamma; a \vdash letx = eint : \sigma}$$

—–

$$\text{T-SELECT}\ \frac{\Gamma; a \vdash x : C \qquad ftype(C, f) = D}{\Gamma; a \vdash x.f : D}$$

—–

$$\text{T-ASSIGN}\ \frac{\begin{array}{cc}\Gamma; a \vdash x : C & ftype(C, f) = D \\ \Gamma; a \vdash y : D' & D' <: D\end{array}}{\Gamma; a \vdash x.f = y : D}$$

—–

$$\text{T-INVOKE}\frac{\begin{array}{cc}\Gamma; a \vdash x : C & mtype(C, m) = \sigma \to \tau \\ \Gamma; a \vdash y : \sigma' & \sigma' <: \sigma \vee \\ \multicolumn{2}{c}{(\sigma = Box[D] \wedge \sigma' = Q \rhd Box[D] \wedge Perm[Q] \in \Gamma)}\end{array}}{\Gamma; a \vdash x.m(y) : \tau}$$

—

$$\text{T-NEW}\frac{a = ocap \implies ocap(C) \qquad \forall var f : \sigma \in \bar{fd}.\exists D.\sigma = D}{\Gamma; a \vdash newC : C}$$

—

$$\text{T-OPEN}\frac{\Gamma; a \vdash x : Q \rhd Box[C] \qquad Perm[Q] \in \Gamma \qquad y : C; ocap \vdash t : \sigma}{\Gamma; a \vdash x.open\{y \Rightarrow t\} : Q \rhd Box[C]}$$

—

$$\text{T-BOX}\frac{ocap(C) \qquad Qfresh \qquad \Gamma; x : Q \rhd Box[C]; Perm[Q]; a \vdash t : \sigma}{\Gamma; a \vdash box[C]\{x \Rightarrow t\} : \bot}$$

—

$$\text{T-CAPTURE}\frac{\begin{array}{cc}\Gamma; a \vdash x : Q \rhd Box[C] & \Gamma; a \vdash y : Q' \rhd Box[D] \\ \{Perm[Q], Perm[Q']\} \subseteq \Gamma & D <: ftype(C, f) \\ \multicolumn{2}{c}{\Gamma\ \{Perm[Q']\}, z : Q \rhd Box[C]; a \vdash t : \sigma}\end{array}}{\Gamma; a \vdash capture(x.f, y)\{z \Rightarrow t\} : \bot}$$

—

$$\text{T-SWAP}\frac{\begin{array}{cc}\Gamma; a \vdash x : Q \rhd Box[C] & \Gamma; a \vdash y : Q' \rhd Box[D'] \\ \{Perm[Q], Perm[Q']\} \subseteq \Gamma & ftype(C, f) = Box[D] \\ D' <: D & Rfresh \\ \multicolumn{2}{c}{\Gamma\ \{Perm[Q']\}, z : R \rhd Box[D], Perm[R]; a \vdash t : \sigma}\end{array}}{\Gamma; a \vdash swap(x.f, y)\{z \Rightarrow t\} : \bot}$$

—

$$\text{T-EMPFS}\frac{}{H \vdash \epsilon}$$

—

$$\text{T-FRAME1}\frac{\begin{array}{cc}\Gamma; a \vdash t : \sigma & l \neq \epsilon \implies \sigma <: C \\ H \vdash \Gamma; L & H \vdash \Gamma; L; P\end{array}}{H \vdash \langle L,\ t,\ P\rangle^l : \sigma}$$

—

$$\text{T-FRAME2}\frac{\begin{array}{cc}\Gamma; x : \tau; a \vdash t : \sigma & l \neq \epsilon \implies \sigma <: C \\ H \vdash \Gamma; L & H \vdash \Gamma; L; P\end{array}}{H \vdash^{\tau}_{x} \langle L,\ t,\ P\rangle^l : \sigma}$$

—

$$\text{T-FRAME-NA}\frac{H \vdash F^{\epsilon} : \sigma \qquad H \vdash FS}{H \vdash F^{\epsilon} \circ FS}$$

—

$$\text{T-FRAME-NA2}\frac{H \vdash^{\tau}_{x} F^{\epsilon} : \sigma \qquad H \vdash FS}{H \vdash^{\tau}_{x} F^{\epsilon} \circ FS}$$

—

$$\text{T-FRAME-A}\frac{H \vdash F^{x} : \sigma \qquad H \vdash^{\sigma}_{x} FS}{H \vdash F^{x} \circ FS}$$

—

$$\text{T-FRAME-A2}\ \frac{H \vdash_x^\tau F^y : \sigma \qquad H \vdash_y^\sigma FS}{H \vdash_x^\tau F^y \circ FS}$$

#### 0.1.2.3 Evaluation

$$\text{E-NULL}\ \frac{}{\begin{array}{c} H,\langle L,\ let x = null int,\ P\rangle^l \\ \rightarrow\ H,\langle L[x \rightarrow null],\ t,\ P\rangle^l \end{array}}$$

$$\text{E-VAR}\ \frac{}{\begin{array}{c} H,\langle L,\ let x = y int,\ P\rangle^l \\ \rightarrow\ H,\langle L[x \rightarrow L(y)],\ t,\ P\rangle^l \end{array}}$$

$$\text{E-SELECT}\ \frac{H(L(y)) = \langle C, FM\rangle \qquad f \in dom(FM)}{\begin{array}{c} H,\langle L,\ let x = y.f int,\ P\rangle^l \\ \rightarrow\ H,\langle L[x \rightarrow FM(f)],\ t,\ P\rangle^l \end{array}}$$

$$\text{E-ASSIGN}\ \frac{\begin{array}{c} L(y) = o \qquad H(o) = \langle C, FM\rangle \\ H' = H[o \rightarrow \langle C, FM[f \rightarrow L(z)]] \end{array}}{\begin{array}{c} H,\langle L,\ let x = y.f = z int,\ P\rangle^l \\ \rightarrow\ H',\langle L,\ let x = z int,\ P\rangle^l \end{array}}$$

$$\text{E-NEW}\ \frac{\begin{array}{c} o \notin dom(H) \qquad fields(C) = \bar{f} \\ H' = H[o \rightarrow \langle C, f \rightarrow null\rangle] \end{array}}{\begin{array}{c} H,\langle L,\ let x = new C int,\ P\rangle^l \\ \rightarrow\ H',\langle L[x \rightarrow o],\ t,\ P\rangle^l \end{array}}$$

$$\text{E-INVOKE}\ \frac{\begin{array}{c} H(L(y)) = \langle C, FM\rangle \qquad mbody(C, m) = x \rightarrow t' \\ L' = L_0[this \rightarrow L(y), x \rightarrow L(z)] \\ P' = \emptyset \vee (L(z) = b(o,p) \wedge p \in P \wedge P' = \{p\}) \end{array}}{\begin{array}{c} H,\langle L,\ let x = y.m(z) int,\ P\rangle^l \circ FS \\ \twoheadrightarrow\ H,\langle L',\ t',\ P'\rangle^x \circ \langle L,\ t,\ P\rangle^l \circ FS \end{array}}$$

$$\text{E-RETURN1}\ \frac{}{\begin{array}{c} H,\langle L,\ x,\ P\rangle^y \circ \langle L',\ t',\ P'\rangle^l \\ \rightarrow\ H,\langle L'[y \rightarrow L(x)],\ t',\ P'\rangle^l \end{array}}$$

$$\text{E-RETURN2}\ \frac{}{\begin{array}{c} H,\langle L,\ x,\ P\rangle^\epsilon \circ \langle L',\ t',\ P'\rangle^l \\ \rightarrow\ H,\langle L',\ t',\ P'\rangle^l \end{array}}$$

$$\text{E-OPEN}\;\frac{L(y) = b(o,p) \quad p \in P \quad L' = [z \to o]}{H,\langle L,\ letx = y.open\{z \Rightarrow t'\}int,\ P\rangle^l \circ FS}$$

$$\twoheadrightarrow\ H,\langle L',\ t',\ \emptyset\rangle^\epsilon \circ \langle L[x \to L(y)],\ t,\ P\rangle^l \circ FS$$

—

$$\text{E-BOX}\;\frac{\begin{array}{c} o \notin dom(H) \qquad fields(C) = \bar{f} \\ H' = H[o \to \langle C, f \to null\rangle] \quad pfresh \end{array}}{H,\langle L,\ box[C]\{x \Rightarrow t\},\ P\rangle^l \circ FS}$$

$$\twoheadrightarrow\ H',\langle L[x \to b(o,p)],\ t,\ P \cup \{p\}\rangle^\epsilon \circ \epsilon$$

—

$$\text{E-CAPTURE}\;\frac{\begin{array}{c} L(x) = b(o,p) \quad L(y) = b(o',p') \quad \{p,p'\} \subseteq P \\ H(o) = \langle C, FM\rangle \quad H' = H[\to \langle C, FM[f \to o']\rangle] \end{array}}{H,\langle L,\ capture(x.f,y)\{z \Rightarrow t\},\ P\rangle^l \circ FS}$$

$$\twoheadrightarrow\ H',\langle L[z \to L(x)],\ t,\ P \setminus \{p'\}\rangle^\epsilon \circ \epsilon$$

—

$$\text{E-SWAP}\;\frac{\begin{array}{c} L(x) = b(o,p) \quad L(y) = b(o',p') \quad \{p,p'\} \subseteq P \\ H(o) = \langle C, FM\rangle \quad FM(f) = o'' \quad p''fresh \\ H' = H[o \to \langle C, FM[f \to o']\rangle] \end{array}}{H,\langle L,\ swap(x.f,y)\{z \Rightarrow t\},\ P\rangle^l \circ FS}$$

$$\twoheadrightarrow\ H',\langle L[z \to b(o'',p'')],\ t,\ (P \setminus \{p'\}) \cup \{p''\}\rangle^\epsilon \circ \epsilon$$

—

#### 0.1.2.4 Definitions

**Definition 1** (Object Type)**.** For an object identifier $o \in dom(H)$ where $H(o) = \langle C, FM\rangle$, $typeof(H,o) := C$

**Definition 2** (Well-typed Heap)**.** A heap $H$ is well-typed, written $\vdash H : \star$, iff

$$\begin{aligned}\forall o \in dom(H).H(o) = \langle C, FM\rangle \implies& \\ &(dom(FM) = fields(C) \wedge \\ &\forall f \in dom(FM).FM(f) = null \vee typeof(H, FM(f)) <: ftype(C,f))\end{aligned} \tag{1}$$

**Definition 3** (Separation)**.** Two object identifiers $o$ and $o'$ are separate in heap $H$, written $sep(H,o,o')$, iff $\forall q, q' \in dom(H).reach(H,o,q) \wedge reach(H,o',q') \implies q \neq q'$.

#### 0.1.2.5 Other

$$\text{ACC-F}\;\frac{x \to o \in L \vee (x \to b(o,p) \in L \wedge p \in P)}{accRoot(o, \langle L,t,P\rangle^l)}$$

$$\text{ACC-FS}\ \frac{accRoot(o, F) \vee accRoot(o, FS)}{accRoot(o, F \circ FS)}$$

$$\text{ISO-FS}\ \frac{\forall o, o' \in dom(H).(accRoot(o, FS) \wedge accRoot(o', FS')) \Rightarrow sep(H, o, o')}{isolated(H, FS, FS')}$$

$$\text{F-OK}\ \frac{\begin{array}{c} boxSep(H, F) \qquad boxObjSep(H, F) \qquad boxOcap(H, F) \\ a = ocap \Longrightarrow globalOcapSep(H, F) \qquad fieldUniqueness(H, F) \end{array}}{H; a \vdash F ok}$$

$$\text{SINGFS-OK}\ \frac{H; a \vdash F ok}{H; a \vdash F \circ \epsilon ok}$$

$$\text{FS-OK}\ \frac{H; b \vdash F^l ok \qquad H; a \vdash FS ok}{H; b \vdash F^l \circ FS ok}$$

#### 0.1.2.6 Predicates

$$\frac{x \to b(o, p) \in L \qquad p \in P}{boxRoot(o, \langle L,\ t,\ P\rangle^l)}$$

$$\frac{boxRoot(o, F)}{boxRoot(o, F \circ \epsilon)}$$

$$\frac{boxRoot(o, F) \vee boxRoot(o, FS)}{boxRoot(o, F \circ FS)}$$

$$\frac{x \to b(o, p) \in L \qquad p \in P}{boxRoot(o, \langle L,\ t,\ P\rangle^l, p)}$$

$$\frac{boxRoot(o, F, p)}{boxRoot(o, F \circ \epsilon, p)}$$

$$\frac{boxRoot(o, F, p) \vee boxRoot(o, FS, p)}{boxRoot(o, F \circ FS, p)}$$

$$\frac{boxRoot(o, FS) \qquad x \to o' \in env(F) \qquad reach(H, o, o')}{openbox(H, o, F, FS)}$$