Mobile Ambients
Syntax, Semantics, and Analysis

René Rydhof Hansen

ASV 2012

1 Syntax

$$
\begin{array}{rcll}
P, Q & ::= & (\nu n)P & \text{restriction} \\
 & | & \mathbf{0} & \text{inactivity} \\
 & | & P \mid Q & \text{composition} \\
 & | & !P & \text{replication} \\
 & | & n[P] & \text{ambient} \\
 & | & M.P & \text{action}
\end{array}
\qquad
\begin{array}{rcll}
M & ::= & \mathtt{in}\ n & \text{enter } n \\
 & | & \mathtt{out}\ n & \text{leave } n \\
 & | & \mathtt{open}\ n & \text{dissolve } n
\end{array}
$$

2 Semantics

2.1 Structural Equivalence

$$P \equiv P \qquad \frac{P \equiv Q}{Q \equiv P} \qquad P \mid \mathbf{0} \equiv P \qquad !\mathbf{0} \equiv \mathbf{0}$$

$$\frac{P \equiv Q \qquad Q \equiv R}{P \equiv R} \qquad \frac{P \equiv Q}{M.P \equiv M.Q} \qquad !P \equiv P \mid !P \qquad (\nu n)\mathbf{0} \equiv \mathbf{0}$$

$$(P \mid Q) \mid R \equiv P \mid (Q \mid R)$$

$$P \mid Q \equiv Q \mid R \qquad \frac{P \equiv Q}{!P \equiv !Q}$$

$$(\nu n)(\nu m)P \equiv (\nu m)(\nu n)P$$

$$\frac{P \equiv Q}{P \mid R \equiv Q \mid R} \qquad \frac{P \equiv Q}{n[P] \equiv n[Q]} \qquad (\nu n)(P \mid Q) \equiv P \mid (\nu n)Q \quad \text{if } n \notin \text{fn}(P)$$

$$\frac{P \equiv Q}{(\nu n)P \equiv (\nu n)Q} \qquad (\nu n)m[P] \equiv m[(\nu n)P] \quad \text{if } n \neq m$$

2.2 Reduction Rules

$$\frac{P \longrightarrow Q}{n[P] \longrightarrow n[Q]} \qquad \frac{P \longrightarrow P'}{P \mid Q \longrightarrow P' \mid Q}$$

$$\frac{P \longrightarrow P'}{(\nu n)P \longrightarrow (\nu n)P'} \qquad \frac{P \equiv P' \qquad P' \longrightarrow Q' \qquad Q' \equiv Q}{P \longrightarrow Q}$$

$$m[\mathtt{in}\ n.P \mid Q] \mid n[R] \quad \longrightarrow \quad n[\, m[P \mid Q] \mid R\,]$$

$$n[\, m[\mathtt{out}\ n.P \mid Q] \mid R\,] \quad \longrightarrow \quad m[P \mid Q] \mid n[R]$$

$$\mathtt{open}\ n.P \mid n[Q] \quad \longrightarrow \quad P \mid Q$$

3 Control Flow Analysis (Flow Logic)

3.1 Representation Function

$$\begin{array}{rcl}
\beta^n(\mathbf{0}) & = & \emptyset \\
\beta^n(!P) & = & \beta^n(P) \\
\beta^n((\nu n)P) & = & \beta^n(P) \\
\beta^n(P \mid Q) & = & \beta^n(P) \cup \beta^n(Q) \\
\beta^n(m[P]) & = & \{(n,m)\} \cup \beta^m(P) \\
\beta^n(\mathtt{in}\ m.P) & = & \{(n, \mathtt{in}\ m)\} \cup \beta^n(P) \\
\beta^n(\mathtt{out}\ m.P) & = & \{(n, \mathtt{out}\ m)\} \cup \beta^n(P) \\
\beta^n(\mathtt{open}\ m.P) & = & \{(n, \mathtt{open}\ m)\} \cup \beta^n(P)
\end{array}$$

3.2 Closure Condition

$$\begin{array}{lll}
\mathcal{C}(I,J) & \text{iff} & \forall p,m,n,I'. \\
& & \quad \{(p,m),(p,n),(m,\mathtt{in}\ n)\} \subseteq I \;\Rightarrow\; \{(n,m)\} \subseteq I \\
& & \wedge\ \{(p,n),(n,m),(m,\mathtt{out}\ n)\} \subseteq I \;\Rightarrow\; \{(p,m)\} \subseteq I \\
& & \wedge\ \{(m,n),(m,\mathtt{open}\ n)\} \subseteq I \;\Rightarrow\; \{(m,x) \mid (n,x) \in I\} \subseteq I
\end{array}$$