A resource analysis of the π-calculus

Aaron Turon
Joint work with Mitchell Wand

Northeastern University

May 27, 2011

$$P \mid \text{new } x.Q$$

$$P \mid \text{new } x.\overbrace{Q}^{x \text{ private}}$$

$$c(y).P \mid \text{new } x.\overline{c}x.Q$$

$$
\begin{aligned}
& c(y).P \mid \text{new } x.\overline{c}x.Q \\
\equiv \quad & \text{new } x.(c(y).P \mid \overline{c}x.Q)
\end{aligned}
$$

$$
\begin{aligned}
& c(y).P \mid \text{new } x.\overline{c}x.Q \\
\equiv \quad & \text{new } x.(c(y).P \mid \overline{c}x.Q) \\
\rightarrow \quad & \text{new } x.(P\{x/y\} \mid Q)
\end{aligned}
$$

Privacy via scope,
mobility via extrusion

$$x := \text{new}\ (0);\ *x := 1$$

$$x := \text{new}\ (0);\ *x := 1,\ \sigma$$

$$
\begin{aligned}
& x := \text{new}\,(0);\ *x := 1,\ \sigma \\
\rightarrow\ & *a := 1,\ \sigma[a \mapsto 0] \qquad (a \notin \sigma)
\end{aligned}
$$

$$
\begin{aligned}
& x := \text{new}\,(0);\ *x := 1,\ \sigma \\
\rightarrow\ & *a := 1,\ \sigma[a \mapsto 0] \qquad (a \notin \sigma)
\end{aligned}
$$

$$\{\text{emp}\}\ x := \text{new}\,(0)\ \{x \mapsto 0\}$$

$$
\begin{aligned}
& x := \mathrm{new}\ (0);\ *x := 1,\ \sigma \\
\to\ \ & *a := 1,\ \sigma[a \mapsto 0] \qquad (a \notin \sigma)
\end{aligned}
$$

$$
\frac{\{\mathrm{emp}\}\ x := \mathrm{new}\ (0)\ \{x \mapsto 0\}}{\{p\}\ x := \mathrm{new}\ (0)\ \{p * x \mapsto 0\}}
$$

Resources, locality, framing

A resource analysis of the π-calculus

- Reconciles allocation, extrusion
  via simple resource model
- Simple new operational semantics
- Simple, *fully abstract* denotational model
- Sketches of a logic, alternative resource models

A resource analysis of the π-calculus

- Reconciles allocation, extrusion
  via simple resource model
- Simple new operational semantics
- Simple, *fully abstract* denotational model
- Sketches of a logic, alternative resource models

$$
\begin{array}{rcl}
P & ::= & \overline{e}e'.P \;\mid\; e(x).P \;\mid\; \text{new } x.P \\
 & \mid & P|Q \;\mid\; \text{rec } X.P \;\mid\; X
\end{array}
$$

$$
e \;::=\; x \;\mid\; c
$$

$$\overline{c}d.P \xrightarrow{c!d} P \qquad \text{new } x.P \xrightarrow{\nu c} P\{c/x\}$$

$$c(x).P \xrightarrow{c?d} P\{d/x\} \qquad \text{rec } X.P \xrightarrow{\tau} P\{\text{rec } X.P/X\}$$

$$\frac{P \xrightarrow{\alpha} P'}{P|Q \xrightarrow{\alpha} P'|Q} \qquad \frac{Q \xrightarrow{\alpha} Q'}{P|Q \xrightarrow{\alpha} P|Q'}$$

$$\frac{P \xrightarrow{\alpha} P' \qquad Q \xrightarrow{\overline{\alpha}} Q'}{P|Q \xrightarrow{\tau} P'|Q'}$$

$$
\begin{aligned}
& \text{new } x.\text{new } y.P \\
\xrightarrow{\nu c}\ & \text{new } y.P\{c/x\} \\
\xrightarrow{\nu c}\ & P\{c/x\}\{c/y\}
\end{aligned}
$$

$$
\begin{aligned}
& \text{new } x.\text{new } y.P \\
\xrightarrow{\nu c} \quad & \text{new } y.P\{c/x\} \\
\xrightarrow{\nu c} \quad & P\{c/x\}\{c/y\}
\end{aligned}
$$

$\Rightarrow$ track channel allocation

$$
\begin{aligned}
& \text{new } x.\text{new } y.P \\
\xrightarrow{\nu c} \quad & \text{new } y.P\{c/x\} \\
\xrightarrow{\nu c} \quad & P\{c/x\}\{c/y\}
\end{aligned}
$$

$\Rightarrow$ track channel allocation

$$
\begin{aligned}
& \text{new } x.\overline{x}d.P \\
\xrightarrow{\nu c} \quad & \overline{c}d.P\{c/x\} \\
\xrightarrow{c!d} \quad & P\{c/x\}
\end{aligned}
$$

$$
\begin{aligned}
& \text{new } x.\text{new } y.P \\
\xrightarrow{\nu c} \quad & \text{new } y.P\{c/x\} \\
\xrightarrow{\nu c} \quad & P\{c/x\}\{c/y\}
\end{aligned}
$$

$\Rightarrow$ track channel allocation

$$
\begin{aligned}
& \text{new } x.\overline{x}d.P \\
\xrightarrow{\nu c} \quad & \overline{c}d.P\{c/x\} \\
\xrightarrow{c!d} \quad & P\{c/x\}
\end{aligned}
$$

$\Rightarrow$ track channel privacy

Resources for π-calculus

$\sigma \in \Sigma \triangleq \textsc{Channel} \rightharpoonup \{\mathrm{pub}, \mathrm{pri}\}$

Resources for π-calculus

$\sigma \in \Sigma \triangleq \textsc{Channel} \rightharpoonup \{\mathsf{pub}, \mathsf{pri}\}$

Action semantics: $\llparenthesis \alpha \rrparenthesis : \Sigma \to \Sigma_{\bot}^{\top}$

$$
\begin{aligned}
\llparenthesis \tau \rrparenthesis \sigma &\triangleq \sigma \\
\llparenthesis \nu c \rrparenthesis \sigma &\triangleq \begin{cases} \sigma[c \mapsto \mathsf{pri}] & c \notin \mathrm{dom}(\sigma) \\ \bot & \text{otherwise} \end{cases}
\end{aligned}
$$

$\bot$ is "impossible", $\top$ is "impermissible"

Action semantics: $(\!|\alpha|\!) : \Sigma \to \Sigma_{\bot}^{\top}$

$$(\!|c!d|\!)\sigma \triangleq \begin{cases} \top & \{c, d\} \nsubseteq \mathrm{dom}(\sigma) \\ \sigma[d \mapsto \mathrm{pub}] & \sigma(c) = \mathrm{pub} \\ \bot & \text{otherwise} \end{cases}$$

$$(\!|c?d|\!)\sigma \triangleq \begin{cases} \top & c \notin \mathrm{dom}(\sigma) \\ \sigma[d \mapsto \mathrm{pub}] & \sigma(c) = \mathrm{pub},\ \sigma(d) \neq \mathrm{pri} \\ \bot & \text{otherwise} \end{cases}$$

Action trace semantics [Brookes 2002]

$$\frac{P \xrightarrow{\alpha} P' \qquad (\!|\alpha|\!)\sigma = \sigma'}{P, \sigma \overset{\alpha}{\rightharpoondown} P', \sigma'} \qquad \frac{P \xrightarrow{\alpha} P' \qquad (\!|\alpha|\!)\sigma = \top}{P, \sigma \overset{\lightning}{\rightharpoondown} 0, \sigma}$$

(no transition for $\bot$)

In the paper: τ, ν steps hidden

$$
\begin{array}{lll}
 & \text{new } x.\text{new } y.P, & \varnothing \\
\xrightarrow{\nu c} & \text{new } y.P\{c/x\}, & [c \mapsto \text{pri}] \\
\not\xrightarrow{\nu c} & &
\end{array}
$$

$$\begin{array}{ll} & \text{new } x.\text{new } y.P, \quad \emptyset \\ \xrightarrow{\nu c} & \text{new } y.P\{c/x\}, \quad [c \mapsto \text{pri}] \\ \stackrel{\nu c}{\not\to} & \end{array}$$

$$\begin{array}{ll} & \text{new } x.\overline{x}d.P, \quad \emptyset \\ \xrightarrow{\nu c} & \overline{c}d.P\{c/x\}, \quad [c \mapsto \text{pri}] \\ \stackrel{c!d}{\not\to} & \end{array}$$

A resource analysis of the π-calculus

- ✓ Reconciles allocation, extrusion
  via simple resource model
- ✓ Simple new operational semantics
- Simple, *fully abstract* denotational model—the payoff
- Sketches of a logic, alternative resource models

Behavior, operationally (safety only)

$$
\begin{aligned}
\mathcal{O}[\![P]\!] &: \textsc{Behavior} \triangleq \Sigma \to 2^{\textsc{Trace}} \\
\mathcal{O}[\![P]\!]\sigma &\triangleq \left\{ t \,:\, P, \sigma \xrightarrow{t}{}^{*} \right\}
\end{aligned}
$$

Behavior, operationally (safety only)

$$\begin{aligned} \mathcal{O}[\![P]\!] &: \textsc{Behavior} \triangleq \Sigma \to 2^{\textsc{Trace}} \\ \mathcal{O}[\![P]\!]\sigma &\triangleq \left\{ t : P, \sigma \xrightarrow{t}{}^{*} \right\} \end{aligned}$$

Goal: compositional, denotational semantics

$[\![P]\!] : \textsc{Environment} \to \textsc{Behavior}$

Note: $\textsc{Behavior}$ is a complete lattice

$$
\begin{array}{rcl}
(\alpha \triangleright B) & : & \textsc{Behavior} \\
(\alpha \triangleright B)(\sigma) & \triangleq & \{\alpha t : (\!|\alpha|\!)\sigma = \sigma',\ t \in B(\sigma')\} \\
& \cup & \{ \lightning : (\!|\alpha|\!)\sigma = \top \} \\
& \cup & \{\epsilon\}
\end{array}
$$

$$[\![\overline{e}e'.P]\!]^{\rho} \triangleq \quad \rho e!\rho e' \triangleright [\![P]\!]^{\rho}$$

$$
\begin{aligned}
[\![\overline{e}e'.P]\!]^{\rho} &\triangleq \rho e!\rho e' \rhd [\![P]\!]^{\rho} \\
[\![e(x).P]\!]^{\rho} &\triangleq \bigsqcup_{c} \rho e?c \rhd [\![P]\!]^{\rho[x\mapsto c]}
\end{aligned}
$$

$$
\begin{aligned}
[\![\overline{e}e'.P]\!]^\rho &\triangleq \rho e!\rho e' \rhd [\![P]\!]^\rho \\
[\![e(x).P]\!]^\rho &\triangleq \textstyle\bigsqcup_c \rho e?c \rhd [\![P]\!]^{\rho[x\mapsto c]} \\
[\![\text{new } x.P]\!]^\rho &\triangleq \textstyle\bigsqcup_c \nu c \rhd [\![P]\!]^{\rho[x\mapsto c]}
\end{aligned}
$$

$$
\begin{aligned}
[\![\overline{e}e'.P]\!]^{\rho} &\triangleq \rho e!\rho e' \triangleright [\![P]\!]^{\rho} \\
[\![e(x).P]\!]^{\rho} &\triangleq \textstyle\bigsqcup_c \rho e?c \triangleright [\![P]\!]^{\rho[x\mapsto c]} \\
[\![\text{new } x.P]\!]^{\rho} &\triangleq \textstyle\bigsqcup_c \nu c \triangleright [\![P]\!]^{\rho[x\mapsto c]}
\end{aligned}
$$

$$
\begin{aligned}
[\![\text{rec } X.P]\!]^{\rho} &\triangleq \mu B. [\![P]\!]^{\rho[X\mapsto B]} \\
[\![X]\!]^{\rho} &\triangleq \rho(X)
\end{aligned}
$$

$$
\begin{aligned}
[\![\overline{e}e'.P]\!]^{\rho} &\triangleq \rho e!\rho e' \rhd [\![P]\!]^{\rho} \\
[\![e(x).P]\!]^{\rho} &\triangleq \textstyle\bigsqcup_c \rho e?c \rhd [\![P]\!]^{\rho[x\mapsto c]} \\
[\![\text{new } x.P]\!]^{\rho} &\triangleq \textstyle\bigsqcup_c \nu c \rhd [\![P]\!]^{\rho[x\mapsto c]}
\end{aligned}
$$

$$
\begin{aligned}
[\![\text{rec } X.P]\!]^{\rho} &\triangleq \mu B.\, [\![P]\!]^{\rho[X\mapsto B]} \\
[\![X]\!]^{\rho} &\triangleq \rho(X)
\end{aligned}
$$

$$
[\![P|Q]\!]^{\rho} \triangleq [\![P]\!]^{\rho} \parallel [\![Q]\!]^{\rho}
$$

$$\text{new } x.(x(y).P \mid \overline{x}c.Q)$$

$$\text{new } x.\ \overbrace{(\underbrace{x(y).P}_{x\ \text{pub}} \mid \underbrace{\overline{x}c.Q}_{x\ \text{pub}})}^{x\ \text{pri}}$$

$$\text{new } x.\overbrace{(\ \underbrace{x(y).P}_{\sigma_1(x)\,=\,\mathsf{pub}}\ \mid\ \underbrace{\overline{x}c.Q}_{\sigma_2(x)\,=\,\mathsf{pub}}\ )}^{\sigma(x)\,=\,\mathsf{pri}}$$

Resource separation

$$
\sigma \in (\sigma_1 \parallel \sigma_2) \triangleq \begin{cases} \mathrm{dom}(\sigma) = \mathrm{dom}(\sigma_1) \cup \mathrm{dom}(\sigma_2) \\ \sigma_1(c) = \mathrm{pri} \implies \begin{array}{l} \sigma(c) = \mathrm{pri}, \\ c \notin \mathrm{dom}(\sigma_2) \end{array} \\ \sigma_2(c) = \mathrm{pri} \implies \begin{array}{l} \sigma(c) = \mathrm{pri}, \\ c \notin \mathrm{dom}(\sigma_1) \end{array} \end{cases}
$$

$$
\begin{array}{lcl}
(B_1 \parallel B_2) & : & \textsc{Behavior} \\
(B_1 \parallel B_2)(\sigma) & \triangleq & \displaystyle\bigcup_{t_i \in B_i(\mathrm{pub}(\sigma))} (t_1 \parallel t_2)(\sigma)
\end{array}
$$

$$
\begin{aligned}
(B_1 \parallel B_2) &: \textsc{Behavior} \\
(B_1 \parallel B_2)(\sigma) &\triangleq \bigcup_{t_i \in B_i(\mathrm{pub}(\sigma))} (t_1 \parallel t_2)(\sigma)
\end{aligned}
$$

$$
\begin{aligned}
(B_1 \parallel B_2) &: \textsc{Behavior} \\
(B_1 \parallel B_2)(\sigma) &\triangleq \bigcup_{t_i \in B_i(\mathsf{pub}(\sigma))} (t_1 \parallel t_2)(\sigma)
\end{aligned}
$$

$$
\begin{aligned}
(B_1 \parallel B_2) \quad &: \quad \textsc{Behavior} \\
(B_1 \parallel B_2)(\sigma) \quad &\triangleq \bigcup_{t_i \in B_i(\mathrm{pub}(\sigma))} (t_1 \parallel t_2)(\sigma)
\end{aligned}
$$

$$
\begin{aligned}
t \parallel u \quad &: \quad \textsc{Behavior} \\
t \parallel u \quad &\triangleq \quad \lambda\sigma.\{\epsilon\} && \text{if } t = \epsilon = u \\
&\sqcup \quad \alpha \triangleright (t' \parallel u) && \text{if } t = \alpha t' \\
&\sqcup \quad \alpha \triangleright (t \parallel u') && \text{if } u = \alpha u' \\
&\sqcup \quad t' \parallel u' && \text{if } t = \alpha t',\ u = \overline{\alpha} u'
\end{aligned}
$$

$$
\begin{aligned}
(B_1 \parallel B_2) \quad &: \quad \textsc{Behavior} \\
(B_1 \parallel B_2)(\sigma) \quad &\triangleq \quad \bigcup_{t_i \in B_i(\mathrm{pub}(\sigma))} (t_1 \parallel t_2)(\sigma)
\end{aligned}
$$

$$
\begin{aligned}
t \parallel u \quad &: \quad \textsc{Behavior} \\
t \parallel u \quad &\triangleq \quad \lambda\sigma.\{\epsilon\} && \text{if } t = \epsilon = u \\
&\sqcup \quad \alpha \rhd (t' \parallel u) && \text{if } t = \alpha t' \\
&\sqcup \quad \alpha \rhd (t \parallel u') && \text{if } u = \alpha u' \\
&\sqcup \quad t' \parallel u' && \text{if } t = \alpha t',\ u = \overline{\alpha} u'
\end{aligned}
$$

$$[\![\text{new } x.(x(y) \mid \overline{x}x)]\!]\,\sigma$$

$$
\begin{aligned}
& [\![\text{new } x.(x(y) \mid \bar{x}x)]\!]\,\sigma \\
= \;& [\![x(y) \mid \bar{x}x]\!]^{[x \mapsto c]}\,\sigma[c \mapsto \text{pri}]
\end{aligned}
$$

$$
\begin{aligned}
& [\![\mathrm{new}\ x.(x(y) \mid \bar{x}x)]\!]\,\sigma \\
= \ & [\![x(y) \mid \bar{x}x]\!]^{[x \mapsto c]}\,\sigma[c \mapsto \mathrm{pri}]
\end{aligned}
$$

$$
[\![x(y)]\!]^{[x \mapsto c]}\,\mathrm{pub}(\sigma)[c \mapsto \mathrm{pub}] \;\approx\; \{\, c?d \,:\, d\ \mathrm{channel} \,\}
$$

$$
\begin{aligned}
& [\![\mathrm{new}\ x.(x(y)\ \mid\ \bar{x}x)]\!]\,\sigma \\
= \ & [\![x(y)\ \mid\ \bar{x}x]\!]^{[x\mapsto c]}\,\sigma[c\mapsto \mathrm{pri}]
\end{aligned}
$$

$$
\begin{aligned}
[\![x(y)]\!]^{[x\mapsto c]}\,\mathrm{pub}(\sigma)[c\mapsto \color{red}{\mathrm{pub}}] &\approx \{c?d\ :\ d\ \mathrm{channel}\ \} \\
[\![\bar{x}x]\!]^{[x\mapsto c]}\,\mathrm{pub}(\sigma)[c\mapsto \color{red}{\mathrm{pub}}] &\approx \{c!c\}
\end{aligned}
$$

$$\begin{aligned}&[\![\text{new } x.(x(y) \mid \bar{x}x)]\!]\,\sigma \\ =\ & [\![x(y) \mid \bar{x}x]\!]^{[x\mapsto c]}\,\sigma[c \mapsto \text{pri}]\end{aligned}$$

$$\begin{aligned}[\![x(y)]\!]^{[x\mapsto c]}\,\text{pub}(\sigma)[c \mapsto \text{pub}] &\approx \{c?d \,:\, d\,\text{channel}\,\} \\ [\![\bar{x}x]\!]^{[x\mapsto c]}\,\text{pub}(\sigma)[c \mapsto \text{pub}] &\approx \{c!c\}\end{aligned}$$

$$(c!c \rhd c?d \rhd 0)(\sigma[c \mapsto \text{pri}]) = \{\epsilon\}$$

$$\begin{aligned}&[\![\mathsf{new}\ x.(x(y)\ \mid\ \overline{x}x)]\!]\,\sigma\\ =\ &[\![x(y)\ \mid\ \overline{x}x]\!]^{[x\mapsto c]}\,\sigma[c\mapsto \mathsf{pri}]\end{aligned}$$

$$\begin{aligned}[\![x(y)]\!]^{[x\mapsto c]}\,\mathsf{pub}(\sigma)[c\mapsto \mathsf{pub}] &\approx \{c?d\ :\ d\,\mathsf{channel}\ \}\\ [\![\overline{x}x]\!]^{[x\mapsto c]}\,\mathsf{pub}(\sigma)[c\mapsto \mathsf{pub}] &\approx \{c!c\}\end{aligned}$$

$$\begin{aligned}(c!c \rhd c?d \rhd 0)(\sigma[c\mapsto \mathsf{pri}]) &= \{\epsilon\}\\ (c?d \rhd c!c \rhd 0)(\sigma[c\mapsto \mathsf{pri}]) &= \{\epsilon\}\end{aligned}$$

$$
\begin{aligned}
& [\![\mathsf{new}\ x.(x(y) \mid \bar{x}x)]\!]\,\sigma \\
= \quad & [\![x(y) \mid \bar{x}x]\!]^{[x\mapsto c]}\,\sigma[c \mapsto \mathsf{pri}]
\end{aligned}
$$

$$
\begin{aligned}
[\![x(y)]\!]^{[x\mapsto c]}\,\mathsf{pub}(\sigma)[c \mapsto \mathsf{pub}] &\approx \{c?d : d\ \text{channel}\} \\
[\![\bar{x}x]\!]^{[x\mapsto c]}\,\mathsf{pub}(\sigma)[c \mapsto \mathsf{pub}] &\approx \{c!c\}
\end{aligned}
$$

$$
\begin{aligned}
(c!c \triangleright c?d \triangleright 0)(\sigma[c \mapsto \mathsf{pri}]) &= \{\epsilon\} \\
(c?d \triangleright c!c \triangleright 0)(\sigma[c \mapsto \mathsf{pri}]) &= \{\epsilon\} \\
(0)(\sigma[c \mapsto \mathsf{pri}]) &= \{\epsilon\}
\end{aligned}
$$

Locality

Theorem. If $\sigma \in \sigma_1 \parallel \sigma_2$ then

- if $(\!|\alpha|\!)\sigma = \top$ then $(\!|\alpha|\!)\sigma_1 = \top$, and
- if $(\!|\alpha|\!)\sigma = \sigma'$ then $(\!|\alpha|\!)\sigma_1 = \top$ or $(\!|\alpha|\!)\sigma_1 = \sigma'_1$ with $\sigma' \in \sigma'_1 \parallel \sigma_2$

Locality

Theorem. If $\sigma \in \sigma_1 \parallel \sigma_2$ then

- if $(\!|\alpha|\!)\sigma = \top$ then $(\!|\alpha|\!)\sigma_1 = \top$, and
- if $(\!|\alpha|\!)\sigma = \sigma'$ then $(\!|\alpha|\!)\sigma_1 = \top$ or $(\!|\alpha|\!)\sigma_1 = \sigma'_1$ with $\sigma' \in \sigma'_1 \parallel \sigma_2$

Communication

Theorem. If $\sigma \in \sigma_1 \parallel \sigma_2$,
$(\!|\alpha|\!)\sigma_1 = \sigma'_1$, and
$(\!|\overline{\alpha}|\!)\sigma_2 = \sigma'_2$
then $\sigma \in \sigma'_1 \parallel \sigma'_2$

Congruence

Theorem. $[\![P]\!] = \mathcal{O}[\![P]\!]$

Congruence

Theorem. $[\![P]\!] = \mathcal{O}[\![P]\!]$

Full abstraction

Corollary. $[\![-]\!]$ is fully abstract

NB: glossing over some (minor) qualifications.

In the paper:

- Allocation, τ steps not observable
- Internal, external choice included
- Liveness: acceptance trace model & full abstraction
- Simple refinement/separation logic
- Additional *fractional* ownership model

Some related work

[**Hoare and O'Hearn**, '08]
"Separation logic semantics for communicating processes"

[**Brookes**, '02–07]
Action traces, concurrent separation logic semantics

[**Stark**, '96], [**Fiore, Moggi, Sangiori**, '96], [**Hennessy**, '02]
Fully abstract models of π via functor categories

A resource analysis of the π-calculus

- ✓ Reconciles allocation, extrusion
  via simple resource model
- ✓ Simple new operational semantics
- ✓ Simple, *fully abstract* denotational model
- Sketches of a logic, alternative resource models

A resource analysis of the π-calculus

- ✓ Reconciles allocation, extrusion
  via simple resource model
- ✓ Simple new operational semantics
- ✓ Simple, *fully abstract* denotational model
- Sketches of a logic, alternative resource models

Thank you