A Calculus of Bounded Capacities

IFIP WG 2.2, Amsterdam 16.05.03

Vladimiro Sassone

with F. Barbanera, M. Bugliesi, M. Dezani

University of Sussex, MYTHS

The Case for Resource Usage Control

Global Computing and Ambient Intelligence involve scenarios where mobile devices enter and exit domains and networks.

Typical Devices:

Today: Smart Cards, Embedded devs (e.g. in cars), Mobile phones, PDAs, Sat navigators, ...

Tomorrow: PAN, VAN, D-ME, P-COM, ...

The Case for Resource Usage Control

Global Computing and Ambient Intelligence involve scenarios where mobile devices enter and exit domains and networks.

Typical Devices:

Today: Smart Cards, Embedded devs (e.g. in cars), Mobile phones, PDAs, Sat navigators, ...

Tomorrow: PAN, VAN, D-ME, P-COM, ...

Requirements:

- Security: Authentication, Privacy, Non Repudiation
- Trust Formation and Management
- Context (e.g. Location) Awareness
- Dynamic Learning and Adaptability
- Policies of Access Control and their Enforcement
- Negotiation of Access, Access Rights, Resource Acquisition
- Protection of Resource Bounds ...

The Case for Resource Usage Control

Global Computing and Ambient Intelligence involve scenarios where mobile devices enter and exit domains and networks.

Typical Devices:

Today: Smart Cards, Embedded devs (e.g. in cars), Mobile phones, PDAs, Sat navigators, ...
Tomorrow: PAN, VAN, D-ME, P-COM, ...

Requirements:

- Security: Authentication, Privacy, Non Repudiation
- Trust Formation and Management
- Context (e.g. Location) Awareness
- Dynamic Learning and Adaptability
- Policies of Access Control and their Enforcement
- Negotiation of Access, Access Rights, Resource Acquisition
- Protection of Resource Bounds ...

Central Notion:
Resource Usage

≪ ⋘ ⋙ ≫

The Case for Resource Usage Control

Global Computing and Ambient Intelligence involve scenarios where mobile devices enter and exit domains and networks.

Typical Devices:

Today: Smart Cards, Embedded devs (e.g. in cars), Mobile phones, PDAs, Sat navigators, . . .

Tomorrow: PAN, VAN, D-ME, P-COM, . . .

Requirements:

- Security: Authentication, Privacy, Non Repudiation
- Trust Formation and Management
- Context (e.g. Location) Awareness
- Dynamic Learning and Adaptability
- Policies of Access Control and their Enforcement
- Negotiation of Access, Access Rights, Resource Acquisition
- Protection of Resource Bounds . . .

Central Notion: Resource Usage

Our Focus: Capacity Bounds Awareness.

BoCa: Bounded Capacities

- Subjective Mobility
- Bounded Capacity Ambients
- Space as a linear co-capability.
- Fine control of capacity.

$$a[\, \mathbf{in}\, b\,.\,P \mid Q\,] \mid b[\, \blacksquare \mid R\,] \searrow \blacksquare \mid b[\, a[\, P \mid Q\,] \mid R\,]$$

subjective move capability

space co-capability

Minimal Desiderata

- Realistic about space occupation. Bigger processes take more space.

$$n[\,\mathbf{in}\, m\,.\,\text{big and fat P}\,] \mid m[\,\_\,] \mid n[\,\mathbf{in}\, m\,.\,\text{small and slim P}\,]$$

- Replication must be handled appropriately

$$a[\,!P\,] = a[\,!P \mid P\,] = a[\,!P \mid P \mid P\,] = a[\,!P \mid P \mid P \mid P\,] = \ldots$$

Allow an analisys of variation in space occupation

- More precisely, control process spawning.

Computation takes space, dynamically, and we'd like to model it.

Fundamentals: Space Conscious Movement

$$a[\, \mathbf{in}\, b \,.\, P \mid Q \,] \mid b[\, \rule{1em}{0.5ex} \mid R \,] \quad \searrow \quad \rule{1em}{0.5ex} \mid b[\, a[\, P \mid Q \,] \mid R \,]$$

$$\rule{1em}{0.5ex} \mid b[\, a[\, \mathbf{out}\, b \,.\, P \mid Q \,] \mid R \,] \quad \searrow \quad a[\, P \mid Q \,] \mid b[\, \rule{1em}{0.5ex} \mid R \,]$$

Fundamentals: Space Conscious Movement

$$a[\,\mathbf{in}\,b\,.\,P \mid Q\,] \mid b[\,\rule{1em}{0.35em} \mid R\,] \quad \searrow \quad \rule{1em}{0.35em} \mid b[\,a[\,P \mid Q\,] \mid R\,]$$

$$\rule{1em}{0.35em} \mid b[\,a[\,\mathbf{out}\,b\,.\,P \mid Q\,] \mid R\,] \quad \searrow \quad a[\,P \mid Q\,] \mid b[\,\rule{1em}{0.35em} \mid R\,]$$

Example: Travelling needs but consumes no space.

$$a[\,\mathbf{in}\,b\,.\,\mathbf{in}\,c\,.\,\mathbf{out}\,c\,.\,\mathbf{out}\,b\,.\,\mathbf{0}\,] \mid b[\,\rule{1em}{0.35em} \mid c[\,\rule{1em}{0.35em}\,]\,]$$

$$\searrow\searrow \rule{1em}{0.35em} \mid b[\,\rule{1em}{0.35em} \mid c[\,a[\,\mathbf{out}\,c\,.\,\mathbf{out}\,b\,.\,\mathbf{0}\,]\,]\,]$$

$$\searrow\searrow a[\,\mathbf{0}\,] \mid b[\,\rule{1em}{0.35em} \mid c[\,\rule{1em}{0.35em}\,]\,]$$

Fundamentals: Space Conscious Movement

- But the size of travellers matters!

$$a^k[\,\mathbf{in}\,b\,.\,P \mid Q\,] \mid b[\,\overbrace{\blacksquare \mid \ldots \mid \blacksquare}^{k \text{ times}} \mid R\,] \searrow \overbrace{\blacksquare \mid \ldots \mid \blacksquare}^{k \text{ times}} \mid b[\,a^k[\,P \mid Q\,] \mid R\,]$$

$$\underbrace{\blacksquare \mid \ldots \mid \blacksquare}_{k \text{ times}} \mid b[\,a^k[\,\mathbf{out}\,b\,.\,P \mid Q\,] \mid R\,] \searrow a^k[\,P \mid Q\,] \mid b[\,\underbrace{\blacksquare \mid \ldots \mid \blacksquare}_{k \text{ times}} \mid R\,]$$

Fundamentals: Space Conscious Movement

- But the size of travellers matters!

$$a^k[\,\mathbf{in}\, b\,.\,P \mid Q\,] \mid b[\,\overbrace{\_ \mid \ldots \mid \_}^{k \text{ times}} \mid R\,] \;\searrow\; \overbrace{\_ \mid \ldots \mid \_}^{k \text{ times}} \mid b[\,a^k[\,P \mid Q\,] \mid R\,]$$

$$\underbrace{\_ \mid \ldots \mid \_}_{k \text{ times}} \mid b[\,a^k[\,\mathbf{out}\, b\,.\,P \mid Q\,] \mid R\,] \;\searrow\; a^k[\,P \mid Q\,] \mid b[\,\underbrace{\_ \mid \ldots \mid \_}_{k \text{ times}} \mid R\,]$$

What is the a^k? A well-formedness annotation measuring the size of P.

It counts spaces: $\mathrm{weight}(\_) = 1$, $\mathrm{weight}(a^k[\,P\,]) = k$ if $\mathrm{weight}(P) = k$, $\perp$ otherwise.

Reduction only for well-formed terms: (1) weights appear as conditions on reductions; (2) the calculus' operators make only sense with type annotations.

Notation. We use $\_^k$ as a shorthand for $\underbrace{\_ \mid \ldots \mid \_}_{k \text{ times}}$.

Fundamentals: Space Conscious Opening

$$\mathbf{opn}\,a\,.\,P \mid a^k[\,\overline{\mathbf{opn}}\,.\,Q \mid R\,] \quad \searrow \quad P \mid Q \mid R$$

A Calculus of Bounded Capacities: Open

Fundamentals: Space Conscious Opening

$$\mathbf{opn}\, a\,.\,P \mid a^k[\,\overline{\mathbf{opn}}\,.\,Q \mid R\,] \quad \searrow \quad P \mid Q \mid R$$

Example: Recovering Mobile Ambients.

$$[\![\, a[\,P\,]\,]\!] \triangleq a^0[\,!\overline{\mathbf{opn}} \mid [\![\,P\,]\!]\,]$$

$$[\![(\boldsymbol{\nu} a)P]\!] \triangleq (\boldsymbol{\nu} a^0)[\![P]\!]$$

$$\ldots$$

≪ ⋘ ⋙ ≫

A Calculus of Bounded Capacities: Spawning

Fundamentals: Space Conscious Process Activation

$$\triangleright^k P \mid \blacksquare^k \quad \equiv \quad P$$

Fundamentals: Space Conscious Process Activation

$$\triangleright^k P \mid \blacksquare^k \quad \equiv \quad P$$

passive process: weighs 0

P weighs k

A Calculus of Bounded Capacities: Spawning

Fundamentals: Space Conscious Process Activation

$$\triangleright^k P \mid \blacksquare^k \equiv P$$

Example: Replication: $!^k \triangleq !\triangleright^k$

$$!\triangleright^k P \mid \blacksquare^k \searrow !\triangleright^k P \mid P$$

Types ensure only 0-weighted processes are replicable: One must use spawning, so that replication needs space proportional to the process' weight.

Fundamentals: Space Conscious Process Activation

$$\triangleright^k P \mid \blacksquare^k \quad \equiv \quad P$$

passive process: weighs 0

P weighs k

Example: Replication: $!^k \triangleq\ !\triangleright^k$

$$!\triangleright^k P \mid \blacksquare^k \quad \searrow \quad !\triangleright^k P \mid P$$

Types ensure only 0-weighted processes are replicable: One must use spawning, so that replication needs space proportional to the process' weight.

Example: Recursion (well, almost):

$$\mathsf{rec}(X^k)P \triangleq (\boldsymbol{\nu} X^k)(!\mathbf{opn}\, X \,.\, \triangleright^k \widehat{P} \mid X[\,\blacksquare^k\,]), \qquad \text{where } \widehat{P} \triangleq P\{X[\,\blacksquare^k\,]/X\}$$

Example: Ambient Spawning

$$\mathsf{spw}^k b[\ P\ ] \triangleq \mathsf{exp}^0[\ \mathbf{out}\, a\,.\,\overline{\mathbf{opn}}\,.\,\triangleright^k b[\ P\ ]\ ]$$

Then,

$$a[\ \mathsf{spw}^k b[\ P\ ]\ |\ Q\ ]\ |\ \blacksquare^k\ |\ \mathbf{opn}\,\mathsf{exp} \quad \searrow \quad a[\ Q\ ]\ |\ b[\ P\ ].$$

The father must provide enough space for the activation, of course.

BoCa: Examples (Open)

Example: Ambient Spawning

$$\mathsf{spw}^k b[\,P\,] \triangleq \mathsf{exp}^0[\,\mathbf{out}\,a\,.\,\overline{\mathbf{opn}}\,.\,\triangleright^k b[\,P\,]\,]$$

Then,

$$a[\,\mathsf{spw}^k b[\,P\,] \mid Q\,] \mid \blacksquare^k \mid \mathbf{opn}\,\mathsf{exp} \quad \searrow \quad a[\,Q\,] \mid b[\,P\,].$$

The father must provide enough space for the activation, of course.

Example: Ambient Renaming

$$\mathsf{a\_be\_b}^k\,.\,P \triangleq \mathsf{spw}^k_a b[\,\blacksquare^k \mid \mathbf{opn}\,a\,] \mid \mathbf{in}\,b\,.\,\overline{\mathbf{opn}}\,.\,P.$$

Then,

$$\blacksquare^k \mid \mathbf{opn}\,x \mid a^k[\,\mathsf{a\_be\_b}^k\,.\,P \mid Q\,] \quad \searrow \quad b[\,P \mid Q\,] \mid \blacksquare^k.$$

Ambient a needs to borrow space to rename itself.

A Calculus of Bounded Capacities: Transfer

Fundamentals: Space Acquisition and Release

$$a^{\hat{}} . P \mid \blacksquare \mid a^k[\ \check{}\ . Q \mid R\ ] \quad \searrow \quad P \mid a^{k+1}[\ Q \mid \blacksquare \mid R\ ]$$

$$a^{k+1}[\ \ll . P \mid \blacksquare \mid S\ ] \mid b^h[\ a\gg . Q \mid R\ ] \quad \searrow \quad a^k[\ P \mid S\ ] \mid b^{h+1}[\ Q \mid \blacksquare \mid R\ ]$$

≪ ⋘ ⋙ ≫

A Calculus of Bounded Capacities: Transfer

Fundamentals: Space Acquisition and Release

$$a^{\wedge} . P \mid \blacksquare \mid a^{k}[\, {}^{\vee} . Q \mid R \,] \quad \searrow \quad P \mid a^{k+1}[\, Q \mid \blacksquare \mid R \,]$$

$$a^{k+1}[\, \ll . P \mid \blacksquare \mid S \,] \mid b^{h}[\, a \gg . Q \mid R \,] \quad \searrow \quad a^{k}[\, P \mid S \,] \mid b^{h+1}[\, Q \mid \blacksquare \mid R \,]$$

Transfer from Child:

$$\text{get\_from\_child}\ a . P \triangleq (\boldsymbol{\nu} n)(\mathbf{opn}\, n . P \mid n[\, a \gg . \overline{\mathbf{opn}} \,])$$

A Calculus of Bounded Capacities: Transfer

Fundamentals: Space Acquisition and Release

$$a^{\hat{}}\,.\,P \mid \blacksquare \mid a^k[\,{}^{\check{}}\,.\,Q \mid R\,] \quad \searrow \quad P \mid a^{k+1}[\,Q \mid \blacksquare \mid R\,]$$

$$a^{k+1}[\,\text{«}\,.\,P \mid \blacksquare \mid S\,] \mid b^h[\,a\text{»}\,.\,Q \mid R\,] \quad \searrow \quad a^k[\,P \mid S\,] \mid b^{h+1}[\,Q \mid \blacksquare \mid R\,]$$

Transfer from Child:

$$\mathsf{get\_from\_child}\ a\,.\,P \triangleq (\boldsymbol{\nu} n)(\mathbf{opn}\,n\,.\,P \mid n[\,a\text{»}.\overline{\mathbf{opn}}\,])$$

Example: A Memory Module

$$\mathsf{memMod} \triangleq \mathsf{mem}[\,\blacksquare^{256MB} \mid !\text{«} \mid !\mathsf{free}\text{»}\,]$$

$$\mathsf{malloc} \triangleq \mathsf{m}[\,!\mathsf{mem}\text{»}\,.\,\mathsf{free}[\,\mathbf{out}\,\mathsf{m}\,.\,\mathsf{m}\text{»}\,.\,\text{«}\,] \mid !\text{«}\,]$$

A Calculus of Bounded Capacities: Transfer

Fundamentals: Space Acquisition and Release

$$a^{\hat{}} \,.\, P \mid \blacksquare \mid a^k[\, ^{\check{}} \,.\, Q \mid R \,] \quad \searrow \quad P \mid a^{k+1}[\, Q \mid \blacksquare \mid R \,]$$

$$a^{k+1}[\, « \,.\, P \mid \blacksquare \mid S \,] \mid b^h[\, a» \,.\, Q \mid R \,] \quad \searrow \quad a^k[\, P \mid S \,] \mid b^{h+1}[\, Q \mid \blacksquare \mid R \,]$$

Transfer from Child:

$$\text{get\_from\_child } a \,.\, P \triangleq (\boldsymbol{\nu} n)(\mathbf{opn}\, n \,.\, P \mid n[\, a» . \overline{\mathbf{opn}} \,])$$

Example: A Memory Module

$$\text{memMod} \triangleq \text{mem}[\, \blacksquare^{256MB} \mid !« \mid !\text{free}» \,]$$

$$\text{malloc} \triangleq \text{m}[\, !\text{mem}» \,.\, \text{free}[\, \mathbf{out}\, \text{m} \,.\, \text{m}» \,.\, « \,] \mid !« \,]$$

$$\text{memMod} \mid \text{malloc} \searrow^{256MB} \text{mem}[\, !« \mid !\text{free}» \,] \mid \text{m}[\, \blacksquare^{256MB} \mid \ldots \,] \searrow^{2\times256MB}$$

$$\text{mem}[\, !« \mid !\text{free}» \,] \mid \text{malloc} \mid \text{free}^{256MB}[\, \blacksquare \mid « \,] \searrow^{256MB} \text{memMod} \mid \text{malloc} \mid \ldots$$

≪ ⋘ ⋙ ≫

On the nature of space

An economic vehicle for multiple concepts

- Available space: $a[\,\blacksquare \mid P\,]$
- Occupied space: $M \centerdot \blacksquare.$ (Notation: $M \centerdot \blacktriangle.$)
- Lost space: $(\boldsymbol{\nu} a)a^k[\,\blacksquare^k\,].$ (Notation: $\mathbf{0}^k.$)

$$\mathsf{destroy}^k \triangleq (\boldsymbol{\nu} a)(\underbrace{a^{\hat{}} \centerdot \ldots \centerdot a^{\hat{}}}_{k \text{ times}}.\mathbf{0} \mid a^0[\,\underbrace{{}^{\check{}} \centerdot \ldots \centerdot {}^{\check{}}}_{k \text{ times}}.\mathbf{0}\,])$$

$$\mathsf{destroy}^k \mid \blacksquare^k \searrow^k \mathbf{0}^k$$

≪ ⋘ ⋙ ≫

A Calculus of Bounded Capabilities: Syntax

$$P ::= \blacksquare \mid \mathbf{0} \mid M \,.\, P \mid P \mid P \mid M[\,P\,] \mid \mathbf{!}P \mid \triangleright^{k} P \mid (\boldsymbol{\nu} n : \pi)P \mid (x : \chi)P \mid \langle M \rangle P$$

$$C ::= \mathbf{in}\, M \mid \mathbf{out}\, M \mid \mathbf{opn}\, M \mid M\hat{\ }\hat{\ } \mid \text{«}$$

$$\overline{C} ::= \overline{\mathbf{opn}} \mid \check{\ }\check{\ } \mid M\text{»}$$

$$M ::= \varepsilon \mid x \mid C \mid \overline{C} \mid M \,.\, M$$

≪ ⋘ ⋙ ≫

A Calculus of Bounded Capabilities: Syntax

$$P ::= \rule{1em}{0.5em} \mid \mathbf{0} \mid M\,.\,P \mid P \mid P \mid M[\,P\,] \mid \mathbf{!}P \mid \triangleright^k P \mid (\boldsymbol{\nu} n : \pi)P \mid (x : \chi)P \mid \langle M \rangle P$$

$$C ::= \mathbf{in}\,M \mid \mathbf{out}\,M \mid \mathbf{opn}\,M \mid M\hat{\ }\hat{\ } \mid «$$

$$\overline{C} ::= \overline{\mathbf{opn}} \mid \check{\ }\check{\ } \mid M»$$

$$M ::= \varepsilon \mid x \mid C \mid \overline{C} \mid M\,.\,M$$

Structural Congruence:

$(|, \mathbf{0})$ is a commutative monoid.

$(\boldsymbol{\nu} a)(P \mid Q) \equiv (\boldsymbol{\nu} a)P \mid Q$ if $a \notin fn(Q)$

$(\boldsymbol{\nu} a)\mathbf{0} \equiv \mathbf{0}$

$(\boldsymbol{\nu} a)\langle M \rangle P \equiv \langle M \rangle (\boldsymbol{\nu} a)P$ if $a \notin fn(P)$

$(\boldsymbol{\nu} a)(\boldsymbol{\nu} b)P \equiv (\boldsymbol{\nu} b)(\boldsymbol{\nu} a)P$

$a[\,(\boldsymbol{\nu} b)P\,] \equiv (\boldsymbol{\nu} b)a[\,P\,]$ if $a \neq b$

$\mathbf{!}P \equiv \mathbf{!}P \mid P$

BoCa: Reduction Semantics

(enter)	$a^k[\,\mathbf{in}\,b\,.\,P \mid Q\,] \mid b[\,\rule{1em}{0.4em}^k \mid R\,]$	$\searrow$	$\rule{1em}{0.4em}^k \mid b[\,a[\,P \mid Q\,] \mid R\,]$
(exit)	$\rule{1em}{0.4em}^k \mid b[\,a^k[\,\mathbf{out}\,b\,.\,P \mid Q\,] \mid R\,]$	$\searrow$	$a^k[\,P \mid Q\,] \mid b[\,\rule{1em}{0.4em}^k \mid R\,]$
(open)	$\mathbf{opn}\,a\,.\,P \mid a[\,\overline{\mathbf{opn}}\,.\,Q \mid R\,]$	$\searrow$	$P \mid Q \mid R$
(tranD)	$a^{\hat{\hat{}}}\,.\,P \mid \rule{1em}{0.4em} \mid a^k[\,\check{\check{}}\,.\,Q \mid R\,]$	$\searrow$	$P \mid a^{k+1}[\,Q \mid \rule{1em}{0.4em} \mid R\,]$
(tranS)	$a^{k+1}[\,\ll\,.\,P \mid \rule{1em}{0.4em} \mid S\,] \mid b^h[\,a\gg\,.\,Q \mid R\,]$	$\searrow$	$a^k[\,P \mid S\,] \mid b^{h+1}[\,Q \mid \rule{1em}{0.4em} \mid R\,]$
(spawn)	$\triangleright^k P \mid \rule{1em}{0.4em}^k$	$\searrow$	P
(comm)	$(x : \chi)P \mid \langle M \rangle Q$	$\searrow$	$P\{x \leftarrow M\} \mid Q$

A System of Capacity Types

Capacity Types: $\phi, \ldots$ are pairs of nats $[n, N]$, with $n \leq N$.

Effect Types $\mathcal{E}, \ldots$ are pairs of nats (d, i), representing decs and incs.

Exchange Types: $\chi ::= \mathsf{Shh} \mid \mathsf{Amb}\langle\sigma, \chi\rangle \mid \mathsf{Cap}\langle\mathcal{E}, \chi\rangle$

Process and **Ambient** and **Capability Types**:

$a : \mathsf{Amb}\langle\phi, \chi\rangle$	a has no less than ϕ_{m} and no more than ϕ_{M} spaces
$P : \mathsf{Proc}\langle k, \mathcal{E}, \chi\rangle$	P weighs k and produces the effect $\mathcal{E}$ on ambients
$C : \mathsf{Cap}\langle\mathcal{E}, \chi\rangle$	C transforms processes adding $\mathcal{E}$ to their effects

Effects and capacities componentwise and are ordered as follows:

$$\sigma \lessdot \phi \equiv \phi_{\mathsf{m}} \leq \sigma_{\mathsf{m}} \text{ and } \sigma_{\mathsf{M}} \leq \phi_{\mathsf{M}},$$

≪ ⋘ ⋙ ≫

A Typing System: Capabilities

(Axiom)

$$\frac{}{\Gamma, a : \mathsf{Amb}\langle \phi, \chi \rangle \vdash a : \mathsf{Amb}\langle \phi, \chi \rangle}$$

(Empty)

$$\frac{}{\Gamma \vdash \varepsilon : \mathsf{Cap}\langle (0,0), \chi \rangle}$$

(In)

$$\frac{\Gamma \vdash M : \mathsf{Amb}\langle \phi, \chi' \rangle}{\Gamma \vdash \mathbf{in}\, M : \mathsf{Cap}\langle (0,0), \chi \rangle}$$

(Out)

$$\frac{\Gamma \vdash M : \mathsf{Amb}\langle \phi, \chi' \rangle}{\Gamma \vdash \mathbf{out}\, M : \mathsf{Cap}\langle (0,0), \chi \rangle}$$

(TranD)

$$\frac{\Gamma \vdash M : \mathsf{Amb}\langle \phi, \chi' \rangle}{\Gamma \vdash M\hat{} : \mathsf{Cap}\langle (0,0), \chi \rangle}$$

(TranS)

$$\frac{}{\Gamma \vdash « : \mathsf{Cap}\langle (1,0), \chi \rangle}$$

(Open)

$$\frac{\Gamma \vdash M : \mathsf{Amb}\langle [n, N], \chi \rangle}{\Gamma \vdash \mathbf{opn}\, M : \mathsf{Cap}\langle (N-n, N-n), \chi \rangle}$$

≪ ⋘ ⋙ ≫

A Typing System: CoCapabilities and Processes

(coTranD)

$$\frac{}{\Gamma \vdash \check{\check{\ }} : \mathsf{Cap}\langle (0,1), \chi \rangle}$$

(coTranS)

$$\frac{\Gamma \vdash M : \mathsf{Amb}\langle \phi, \chi' \rangle}{\Gamma \vdash M\text{»} : \mathsf{Cap}\langle (0,1), \chi \rangle}$$

(coOpen)

$$\frac{}{\Gamma \vdash \overline{\mathbf{opn}} : \mathsf{Cap}\langle (0,0), \chi \rangle}$$

(Composition)

$$\frac{\Gamma \vdash M : \mathsf{Cap}\langle \mathcal{E}, \chi \rangle \quad \Gamma \vdash M' : \mathsf{Cap}\langle \mathcal{E}', \chi \rangle}{\Gamma \vdash M.M' : \mathsf{Cap}\langle \mathcal{E} + \mathcal{E}', \chi \rangle}$$

(Slot)

$$\frac{}{\Gamma \vdash \rule{1em}{0.3em} : \mathsf{Proc}\langle 1, (0,0), \chi \rangle}$$

(Zero)

$$\frac{}{\Gamma \vdash \mathbf{0} : \mathsf{Proc}\langle 0, (0,0), \chi \rangle}$$

(Input)

$$\frac{\Gamma, x : \chi \vdash P : \mathsf{Proc}\langle k, \mathcal{E}, \chi \rangle}{\Gamma \vdash (x : \chi)P : \mathsf{Proc}\langle k, \mathcal{E}, \chi \rangle}$$

(Output)

$$\frac{\Gamma \vdash M : \chi \quad \Gamma \vdash P : \mathsf{Proc}\langle k, \mathcal{E}, \chi \rangle}{\Gamma \vdash \langle M \rangle P : \mathsf{Proc}\langle k, \mathcal{E}, \chi \rangle}$$

A Typing System: Processes

(Prefix)
$$\frac{\Gamma \vdash M : \mathsf{Cap}\langle \mathcal{E}, \chi \rangle \quad \Gamma \vdash P : \mathsf{Proc}\langle k, \mathcal{E}', \chi \rangle}{\Gamma \vdash M \,.\, P : \mathsf{Proc}\langle k, \mathcal{E} + \mathcal{E}', \chi \rangle}$$

(Replication)
$$\frac{\Gamma \vdash P : \mathsf{Proc}\langle 0, (0,0), \chi \rangle}{\Gamma \vdash\, !P : \mathsf{Proc}\langle 0, (0,0), \chi \rangle}$$

(New)
$$\frac{\Gamma, a : \mathsf{Amb}\langle \phi, \chi \rangle \vdash P : \mathsf{Proc}\langle k, \mathcal{E}, \chi' \rangle}{\Gamma \vdash (\boldsymbol{\nu} a : \mathsf{Amb}\langle \phi, \chi \rangle) P : \mathsf{Proc}\langle k, \mathcal{E}, \chi' \rangle}$$

(Spawn)
$$\frac{\Gamma \vdash P : \mathsf{Proc}\langle k, \mathcal{E}, \chi \rangle}{\Gamma \vdash \triangleright^{k} P : \mathsf{Proc}\langle 0, \mathcal{E}, \chi \rangle}$$

(Parallel)
$$\frac{\Gamma \vdash P : \mathsf{Proc}\langle k, \mathcal{E}, \chi \rangle \quad \Gamma \vdash Q : \mathsf{Proc}\langle k', \mathcal{E}', \chi \rangle}{\Gamma \vdash P \mid Q : \mathsf{Proc}\langle k + k', \mathcal{E} + \mathcal{E}', \chi \rangle}$$

(Ambient)
$$\frac{\Gamma \vdash M : \mathsf{Amb}\langle [n, N], \chi \rangle \quad \Gamma \vdash P : \mathsf{Proc}\langle k, (d, i), \chi \rangle \quad n \leq k - d \quad k + i \leq N}{\Gamma \vdash M^{k}[\, P \,] : \mathsf{Proc}\langle k, (0,0), \chi' \rangle}$$

A Calculus of Bounded Capabilities

Thm: Subject Reduction

If $\Gamma \vdash P : \mathtt{Proc}\langle k, \mathcal{E}, \chi\rangle$ and $P \searrow Q$ then $\Gamma \vdash Q : \mathtt{Proc}\langle k, \mathcal{E}', \chi\rangle$ for some $\mathcal{E}' \lessdot \mathcal{E}$.

Thm: Subject Reduction

If $\Gamma \vdash P : \mathtt{Proc}\langle k, \mathcal{E}, \chi \rangle$ and $P \searrow Q$ then $\Gamma \vdash Q : \mathtt{Proc}\langle k, \mathcal{E}', \chi \rangle$ for some $\mathcal{E}' \lessdot \mathcal{E}$.

The missing bit:

Grave interferences in the use of spaces

$$a[\, \mathbf{in}\, b\,] \mid b[\, \triangleright P \mid \rule{1em}{0.3em} \mid a[\, c[\, \mathbf{out}\, a\,]\,]\,]$$

Thm: Subject Reduction

If $\Gamma \vdash P : \mathsf{Proc}\langle k, \mathcal{E}, \chi \rangle$ and $P \searrow Q$ then $\Gamma \vdash Q : \mathsf{Proc}\langle k, \mathcal{E}', \chi \rangle$ for some $\mathcal{E}' \lessdot \mathcal{E}$.

The missing bit:

Grave interferences in the use of spaces

$$a[\ \mathbf{in}\, b\ ] \mid b[\ \triangleright P \mid \blacksquare \mid a[\ c[\ \mathbf{out}\, a\ ]\ ]\ ]$$

Thm: Subject Reduction

If $\Gamma \vdash P : \mathsf{Proc}\langle k, \mathcal{E}, \chi \rangle$ and $P \searrow Q$ then $\Gamma \vdash Q : \mathsf{Proc}\langle k, \mathcal{E}', \chi \rangle$ for some $\mathcal{E}' \lessdot \mathcal{E}$.

The missing bit:

Grave interferences in the use of spaces

$$a[\,\mathbf{in}\, b\,] \mid b[\,\triangleright P \mid \rule{1em}{0.3em} \mid a[\,c[\,\mathbf{out}\, a\,]\,]\,]$$

$$\mathsf{rec}(X^k)P \triangleq (\boldsymbol{\nu} X^k)(\mathbf{!opn}\, X \,.\, \triangleright^k \widehat{P} \mid X[\,\rule{1em}{0.3em}^{\,k}\,])$$

Thm: Subject Reduction

If $\Gamma \vdash P : \mathsf{Proc}\langle k, \mathcal{E}, \chi \rangle$ and $P \searrow Q$ then $\Gamma \vdash Q : \mathsf{Proc}\langle k, \mathcal{E}', \chi \rangle$ for some $\mathcal{E}' \lessdot \mathcal{E}$.

The missing bit:

Grave interferences in the use of spaces

$$a[\,\mathbf{in}\, b\,] \mid b[\, \triangleright P \mid \blacksquare \mid a[\, c[\,\mathbf{out}\, a\,]\,]\,]$$

$$\mathsf{rec}(X^k)P \triangleq (\boldsymbol{\nu} X^k)(\mathbf{!opn}\, X\,.\triangleright^k \widehat{P} \mid X[\,\blacksquare^k\,])$$

$$\searrow (\boldsymbol{\nu} X^k)(\mathbf{!opn}\, X\,.\triangleright^k \widehat{P} \mid \mathbf{opn}\, X\,.\triangleright^k \widehat{P} \mid X[\,\blacksquare^k\,])$$

Thm: Subject Reduction

If $\Gamma \vdash P : \mathsf{Proc}\langle k, \mathcal{E}, \chi\rangle$ and $P \searrow Q$ then $\Gamma \vdash Q : \mathsf{Proc}\langle k, \mathcal{E}', \chi\rangle$ for some $\mathcal{E}' \lessdot \mathcal{E}$.

The missing bit:

Grave interferences in the use of spaces

$$a[\,\mathbf{in}\, b\,] \mid b[\,\triangleright P \mid \blacksquare \mid a[\,c[\,\mathbf{out}\, a\,]\,]\,]$$

$$\mathsf{rec}(X^k)P \triangleq (\boldsymbol{\nu} X^k)(\mathbf{!opn}\, X \,.\, \triangleright^k \widehat{P} \mid X[\,\blacksquare^k\,])$$

$$\searrow (\boldsymbol{\nu} X^k)(\mathbf{!opn}\, X \,.\, \triangleright^k \widehat{P} \mid \mathbf{opn}\, X \,.\, \triangleright^k \widehat{P} \mid X[\,\blacksquare^k\,])$$

$$\searrow (\boldsymbol{\nu} X^k)(\mathbf{!opn}\, X \,.\, \triangleright^k \widehat{P} \mid \triangleright^k \widehat{P} \mid \blacksquare^k)$$

Thm: Subject Reduction

If $\Gamma \vdash P : \mathtt{Proc}\langle k, \mathcal{E}, \chi\rangle$ and $P \searrow Q$ then $\Gamma \vdash Q : \mathtt{Proc}\langle k, \mathcal{E}', \chi\rangle$ for some $\mathcal{E}' \lessdot \mathcal{E}$.

The missing bit:

Grave interferences in the use of spaces

$$a[\,\mathbf{in}\,b\,] \mid b[\,\triangleright P \mid \blacksquare \mid a[\,c[\,\mathbf{out}\,a\,]\,]\,]$$

$$\mathtt{rec}(X^k)P \triangleq (\boldsymbol{\nu} X^k)(\mathbf{!opn}\,X\,.\,\triangleright^k \widehat{P} \mid X[\,\blacksquare^k\,])$$

$$\searrow (\boldsymbol{\nu} X^k)(\mathbf{!opn}\,X\,.\,\triangleright^k \widehat{P} \mid \mathbf{opn}\,X\,.\,\triangleright^k \widehat{P} \mid X[\,\blacksquare^k\,])$$

$$\searrow (\boldsymbol{\nu} X^k)(\mathbf{!opn}\,X\,.\,\triangleright^k \widehat{P} \mid \triangleright^k \widehat{P}) \mid \blacksquare^k \quad \text{Oooops}$$

Control Space Usage: Named Slots

$P ::= \blacksquare_a \mid a \triangleright^k P \mid \cdots$

(spawn) $a \triangleright^k P \mid \blacksquare_a^k \searrow P$

Control Space Usage: Named Slots

$P ::= \blacksquare_a \mid a \triangleright^k P \mid \cdots$ (spawn) $a \triangleright^k P \mid \blacksquare^k_a \searrow P$

Example: Renaming slots

$$\{{}^{x}/_{y}\}_k \cdot P \triangleq y \triangleright^k (\blacksquare^k_x \mid P)$$

Then, $\blacksquare^k_y \mid \{{}^{x}/_{y}\}_k \cdot P \searrow \blacksquare^k_x \mid P$

Control Space Usage: Named Slots

$P ::= \blacksquare_a \mid a \triangleright^k P \mid \cdots$ (spawn) $a \triangleright^k P \mid \blacksquare_a^k \searrow P$

Example: Renaming slots

$$\{^x/_y\}_k \cdot P \triangleq y \triangleright^k (\blacksquare_x^k \mid P)$$

Then, $\blacksquare_y^k \mid \{^x/_y\}_k \cdot P \searrow \blacksquare_x^k \mid P$

Example: Recursion (now right):

$$\mathrm{rec}(X^k)P \triangleq (\boldsymbol{\nu} X)(!X \triangleright^k \widehat{P} \mid \blacksquare_X^k), \quad \text{where } \widehat{P} \triangleq P\{\blacksquare_X^k / X\}$$

Control Space Usage: Named Slots

$P ::= \blacksquare_a \mid a\triangleright^k P \mid \cdots$ (spawn) $a\triangleright^k P \mid \blacksquare_a^k \searrow P$

Example: Renaming slots

$$\{^x/_y\}_k \,.\, P \triangleq y\triangleright^k(\blacksquare_x^k \mid P)$$

Then, $\blacksquare_y^k \mid \{^x/_y\}_k \,.\, P \searrow \blacksquare_x^k \mid P$

Example: Recursion (now right):

$$\mathrm{rec}(X^k)P \triangleq (\boldsymbol{\nu} X)(\mathbf{!}X\triangleright^k \widehat{P} \mid \blacksquare_X^k), \quad \text{where } \widehat{P} \triangleq P\{\blacksquare_X^k / X\}$$

Example: Deriving Named Slots

$$\blacksquare_a \triangleq a[\, \ll \mid \blacksquare \,]$$

$$a\triangleright^k P \triangleq (\boldsymbol{\nu} n)(n[\, a^k \gg . \triangleright^k \overline{\mathbf{opn}} \,.\, P \,] \mid \mathbf{opn}\, n)$$

Conclusions

Typed Barbed Congruence:

$$P \downarrow_b \quad \text{if} \quad P \equiv (\boldsymbol{\nu}\vec{x})b[\,\blacksquare \mid Q'\,] \mid Q'', \quad \text{where } b \notin \vec{x}$$

$$P \Downarrow_b \quad \text{if} \quad P \searrow^{*} \downarrow_b$$

This is sufficient to capture important differences.

Labelled Transition System: Easy enough.

Conclusions

Typed Barbed Congruence:

$$P \downarrow_b \quad \text{if} \quad P \equiv (\boldsymbol{\nu}\vec{x})b[\,\_\,|\,Q'\,]\,|\,Q'', \quad \text{where } b \notin \vec{x}$$

$$P \Downarrow_b \quad \text{if} \quad P \searrow^{*} \downarrow_b$$

This is sufficient to capture important differences.

Labelled Transition System: Easy enough.

Yet to be done:

- In the large: Resource bounds negotiation and enforcement in GC.
- In the small: Expressiveness of BoCa; Equational theory; Smarter types; . . .
- In general: A lot to be done. . .