

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,



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

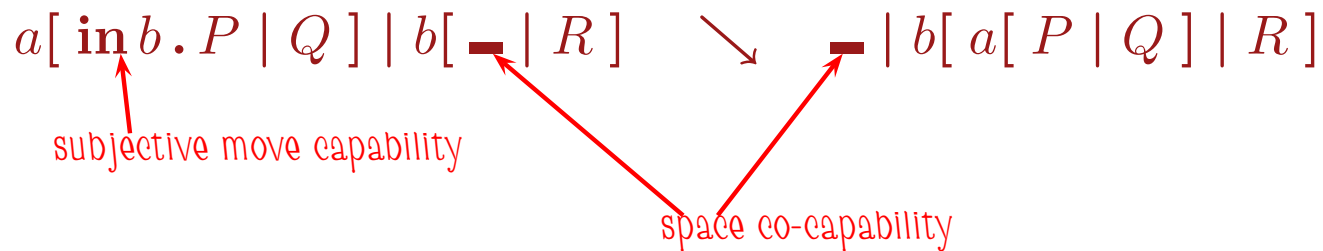
Our Focus: Capacity Bounds Awareness.



Dimensions, Capacities, Mobility

BoCa: Bounded Capacities

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



Minimal Desiderata

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

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

- **Replication** must be handled appropriately

$$a[!P] = a[!P \mid P] = a[!P \mid P \mid P] = a[!P \mid P \mid P \mid P] = \dots$$

Allow an analysis of variation in space occupation

- More precisely, control **process spawning**.

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

A Calculus of Bounded Capacities: Movement

Fundamentals: Space Conscious Movement

$$\begin{array}{l} a[\mathbf{in} b.P \mid Q] \mid b[\mathbf{-} \mid R] \quad \searrow \quad \mathbf{-} \mid b[a[P \mid Q] \mid R] \\ \mathbf{-} \mid b[a[\mathbf{out} b.P \mid Q] \mid R] \quad \searrow \quad a[P \mid Q] \mid b[\mathbf{-} \mid R] \end{array}$$

A Calculus of Bounded Capacities: Movement

Fundamentals: Space Conscious Movement

$$\begin{array}{l} a[\mathbf{in} b.P \mid Q] \mid b[\mathbf{-} \mid R] \quad \searrow \quad \mathbf{-} \mid b[a[P \mid Q] \mid R] \\ \mathbf{-} \mid b[a[\mathbf{out} b.P \mid Q] \mid R] \quad \searrow \quad a[P \mid Q] \mid b[\mathbf{-} \mid R] \end{array}$$

Example: Travelling needs but consumes no space.

$$\begin{array}{l} a[\mathbf{in} b.\mathbf{in} c.\mathbf{out} c.\mathbf{out} b.\mathbf{0}] \mid b[\mathbf{-} \mid c[\mathbf{-}]] \\ \searrow \searrow \mathbf{-} \mid b[\mathbf{-} \mid c[a[\mathbf{out} c.\mathbf{out} b.\mathbf{0}]]] \\ \searrow \searrow a[\mathbf{0}] \mid b[\mathbf{-} \mid c[\mathbf{-}]] \end{array}$$

A Calculus of Bounded Capacities: Well-formedness

Fundamentals: Space Conscious Movement

● But the **size** of travellers matters!

$$\begin{array}{l} a^k [\mathbf{in} b . P \mid Q] \mid b[\overbrace{- \mid \dots \mid -}^{k \text{ times}} \mid R] \\ \underbrace{- \mid \dots \mid -}_{k \text{ times}} \mid b[a^k [\mathbf{out} b . P \mid Q] \mid R] \end{array} \quad \searrow \quad \begin{array}{l} \overbrace{- \mid \dots \mid -}^{k \text{ times}} \mid b[a^k [P \mid Q] \mid R] \\ a^k [P \mid Q] \mid b[\underbrace{- \mid \dots \mid -}_{k \text{ times}} \mid R] \end{array}$$

A Calculus of Bounded Capacities: Well-formedness

Fundamentals: Space Conscious Movement

● But the **size** of travellers matters!

$$\begin{array}{ccc}
 a^k [\mathbf{in} \ b . P \mid Q] \mid b[\overbrace{_ \mid \dots \mid _}^{k \text{ times}} \mid R] & \searrow & \overbrace{_ \mid \dots \mid _}^{k \text{ times}} \mid b[a^k [P \mid Q] \mid R] \\
 \underbrace{_ \mid \dots \mid _}_{k \text{ times}} \mid b[a^k [\mathbf{out} \ b . P \mid Q] \mid R] & \searrow & a^k [P \mid Q] \mid b[\underbrace{_ \mid \dots \mid _}_{k \text{ times}} \mid R]
 \end{array}$$

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

It counts spaces: $\text{weight}(_) = 1$, $\text{weight}(a^k [P]) = k$ if $\text{weight}(P) = k$, \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 $\underbrace{_ \mid \dots \mid _}_{k \text{ times}}$.

A Calculus of Bounded Capacities: Open

Fundamentals: Space Conscious Opening

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



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.

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

$$\llbracket (\nu a) P \rrbracket \triangleq (\nu a^0) \llbracket P \rrbracket$$

...

A Calculus of Bounded Capacities: Spawning

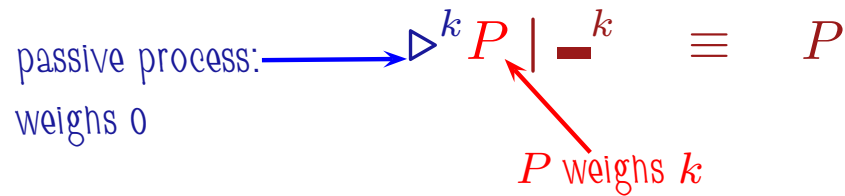
Fundamentals: Space Conscious Process Activation

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



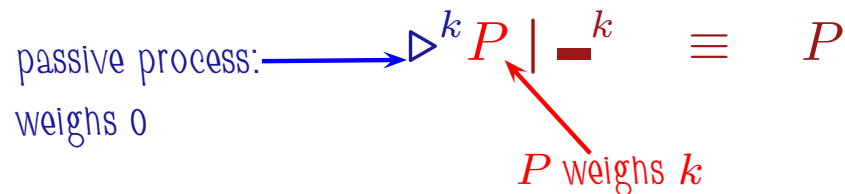
A Calculus of Bounded Capacities: Spawning

Fundamentals: Space Conscious Process Activation



A Calculus of Bounded Capacities: Spawning

Fundamentals: Space Conscious Process Activation



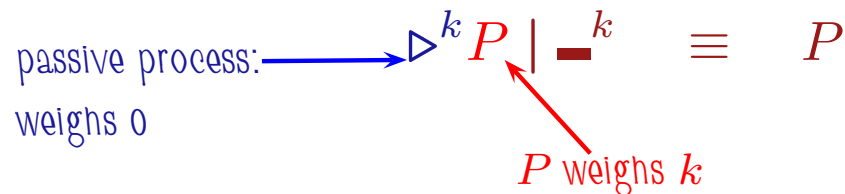
Example: Replication: $!^k \triangleq !\triangleright^k$

$$!\triangleright^k P \mid \bar{_}^k \searrow !\triangleright^k P \mid P$$

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

A Calculus of Bounded Capacities: Spawning

Fundamentals: Space Conscious Process Activation



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

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

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

Example: Recursion (well, almost):

$$\text{rec}(X^k)P \triangleq (\nu X^k)(!\text{opn } X . \triangleright^k \hat{P} \mid X[\dashv^k]), \quad \text{where } \hat{P} \triangleq P\{X[\dashv^k]/X\}$$



BoCa: Examples (Open)

Example: Ambient Spawning

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

Then,

$$a[\text{spw}^k b[P] \mid Q] \mid \text{---}^k \mid \text{opn exp} \quad \searrow \quad a[Q] \mid b[P].$$

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



BoCa: Examples (Open)

Example: Ambient Spawning

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

Then,

$$a[\text{spw}^k b[P] | Q] | \underline{-}^k | \text{opn } \text{exp} \quad \searrow \quad a[Q] | b[P] .$$

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

Example: Ambient Renaming

$$a_be_b^k . P \triangleq \text{spw}_a^k b[\underline{-}^k | \text{opn } a] | \text{in } b . \overline{\text{opn}} . P .$$

Then,

$$\underline{-}^k | \text{opn } x | a^k [a_be_b^k . P | Q] \quad \searrow \quad b[P | Q] | \underline{-}^k .$$

Ambient a needs to **borrow** space to rename itself.

A Calculus of Bounded Capacities: Transfer

Fundamentals: Space Acquisition and Release

$$a^{\hat{}} \cdot P \mid _ \mid a^k [\checkmark \cdot Q \mid R] \quad \searrow \quad P \mid a^{k+1} [Q \mid _ \mid R]$$

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



A Calculus of Bounded Capacities: Transfer

Fundamentals: Space Acquisition and Release

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

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

Transfer from Child:

$$\text{get_from_child } a . P \triangleq (\nu n)(\text{opn } n . P \mid n [a \gg . \overline{\text{opn}}])$$



A Calculus of Bounded Capacities: Transfer

Fundamentals: Space Acquisition and Release

$$\begin{aligned} a^{\hat{}} . P \mid _ \mid a^k [\checkmark . Q \mid R] &\searrow P \mid a^{k+1} [Q \mid _ \mid R] \\ a^{k+1} [\ll . P \mid _ \mid S] \mid b^h [a \gg . Q \mid R] &\searrow a^k [P \mid S] \mid b^{h+1} [Q \mid _ \mid R] \end{aligned}$$

Transfer from Child:

$$\text{get_from_child } a . P \triangleq (\nu n)(\text{opn } n . P \mid n [a \gg . \overline{\text{opn}}])$$

Example: A Memory Module

$$\text{memMod} \triangleq \text{mem} [_^{256MB} \mid !\ll \mid !\text{free}\gg]$$

$$\text{malloc} \triangleq m [!\text{mem}\gg . \text{free} [\text{out } m . m \gg . \ll] \mid !\ll]$$

A Calculus of Bounded Capacities: Transfer

Fundamentals: Space Acquisition and Release

$$\begin{aligned} a^{\hat{}} . P \mid _ \mid a^k [\checkmark . Q \mid R] &\searrow P \mid a^{k+1} [Q \mid _ \mid R] \\ a^{k+1} [\ll . P \mid _ \mid S] \mid b^h [a \gg . Q \mid R] &\searrow a^k [P \mid S] \mid b^{h+1} [Q \mid _ \mid R] \end{aligned}$$

Transfer from Child:

$$\text{get_from_child } a . P \triangleq (\nu n)(\text{opn } n . P \mid n [a \gg . \overline{\text{opn}}])$$

Example: A Memory Module

$$\text{memMod} \triangleq \text{mem} [_^{256MB} \mid !\ll \mid !\text{free}\gg]$$

$$\text{malloc} \triangleq m [!\text{mem}\gg . \text{free} [\text{out } m . m \gg . \ll] \mid !\ll]$$

$$\text{memMod} \mid \text{malloc} \searrow^{256MB} \text{mem} [!\ll \mid !\text{free}\gg] \mid m [_^{256MB} \mid \dots] \searrow^{2 \times 256MB}$$

$$\text{mem} [!\ll \mid !\text{free}\gg] \mid \text{malloc} \mid \text{free}^{256MB} [_ \mid \ll] \searrow^{256MB} \text{memMod} \mid \text{malloc} \mid \dots$$



On the nature of space

An economic vehicle for multiple concepts

- Available space: $a[_ | P]$
- Occupied space: $M . _ .$ (Notation: $M . \blacktriangle .$)
- Lost space: $(\nu a) a^k [_ ^k] .$ (Notation: $\mathbf{0}^k .$)

$$\text{destroy}^k \triangleq (\nu a) (\underbrace{\hat{a} \dots \hat{a}}_{k \text{ times}} . \mathbf{0} | a^0 [\underbrace{\check{\dots} \check{\dots}}_{k \text{ times}} . \mathbf{0}])$$

$$\text{destroy}^k | _ ^k \searrow^k \mathbf{0}^k$$

A Calculus of Bounded Capabilities: Syntax

$$P ::= \mathbf{-} \mid \mathbf{0} \mid M . P \mid P \mid P \mid M[P] \mid !P \mid \triangleright^k P \mid (\nu n : \pi)P \mid (x : \chi)P \mid \langle M \rangle P$$
$$C ::= \mathbf{in} M \mid \mathbf{out} M \mid \mathbf{opn} M \mid M^\wedge \mid \ll$$
$$\bar{C} ::= \overline{\mathbf{opn}} \mid \checkmark \mid M \gg$$
$$M ::= \varepsilon \mid x \mid C \mid \bar{C} \mid M . M$$

A Calculus of Bounded Capabilities: Syntax

$$P ::= \mathbf{-} \mid \mathbf{0} \mid M . P \mid P \mid P \mid M[P] \mid !P \mid \triangleright^k P \mid (\nu n : \pi)P \mid (x : \chi)P \mid \langle M \rangle P$$
$$C ::= \mathbf{in} M \mid \mathbf{out} M \mid \mathbf{opn} M \mid M^\hat{\ } \mid \ll$$
$$\bar{C} ::= \overline{\mathbf{opn}} \mid \check{\ } \mid M \gg$$
$$M ::= \varepsilon \mid x \mid C \mid \bar{C} \mid M . M$$

Structural Congruence:

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

$$(\nu a)(P \mid Q) \equiv (\nu a)P \mid Q \quad \text{if } a \notin \text{fn}(Q)$$
$$(\nu a)\mathbf{0} \equiv \mathbf{0}$$
$$(\nu a)\langle M \rangle P \equiv \langle M \rangle (\nu a)P \quad \text{if } a \notin \text{fn}(P)$$
$$(\nu a)(\nu b)P \equiv (\nu b)(\nu a)P$$
$$a[(\nu b)P] \equiv (\nu b)a[P] \quad \text{if } a \neq b$$
$$!P \equiv !P \mid P$$


BoCa: Reduction Semantics

$$(enter) \quad a^k[\mathbf{in} b . P \mid Q] \mid b[\mathbf{-}^k \mid R] \quad \searrow \quad \mathbf{-}^k \mid b[a[P \mid Q] \mid R]$$

$$(exit) \quad \mathbf{-}^k \mid b[a^k[\mathbf{out} b . P \mid Q] \mid R] \quad \searrow \quad a^k[P \mid Q] \mid b[\mathbf{-}^k \mid R]$$

$$(open) \quad \mathbf{opn} a . P \mid a[\overline{\mathbf{opn}} . Q \mid R] \quad \searrow \quad P \mid Q \mid R$$

$$(tranD) \quad a^{\hat{}} . P \mid \mathbf{-} \mid a^k[\check{} . Q \mid R] \quad \searrow \quad P \mid a^{k+1}[Q \mid \mathbf{-} \mid R]$$

$$(trans) \quad a^{k+1}[\ll . P \mid \mathbf{-} \mid S] \mid b^h[a \gg . Q \mid R] \quad \searrow \quad a^k[P \mid S] \mid b^{h+1}[Q \mid \mathbf{-} \mid R]$$

$$(spawn) \quad \triangleright^k P \mid \mathbf{-}^k \quad \searrow \quad P$$

$$(comm) \quad (x : \chi)P \mid \langle M \rangle Q \quad \searrow \quad P\{x \leftarrow M\} \mid Q$$

A System of Capacity Types

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

Effect Types \mathcal{E}, \dots are pairs of nats (d, i) , representing dees and ins.

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

Process and Ambient and Capability Types:

$a : \text{Amb}\langle\phi, \chi\rangle$ a has no less than ϕ_m and no more than ϕ_M spaces

$P : \text{Proc}\langle k, \mathcal{E}, \chi\rangle$ P weighs k and produces the effect \mathcal{E} on ambients

$C : \text{Cap}\langle\mathcal{E}, \chi\rangle$ C transforms processes adding \mathcal{E} to their effects

Effects and capacities componentwise and are ordered as follows:

$$\sigma \triangleleft \phi \equiv \phi_m \leq \sigma_m \text{ and } \sigma_M \leq \phi_M,$$

A Typing System: Capabilities

(Axiom)

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

(Empty)

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

(In)

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

(Out)

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

(TranD)

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

(Trans)

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

(Open)

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

A Typing System: CoCapabilities and Processes

(coTranD)

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

(coOpen)

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

(Slot)

$$\frac{}{\Gamma \vdash \mathbf{-} : \text{Proc}\langle 1, (0, 0), \chi\rangle}$$

(Input)

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

(coTrans)

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

(Composition)

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

(Zero)

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

(Output)

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

A Typing System: Processes

(Prefix)

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

(Replication)

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

(New)

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

(Spawn)

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

(Parallel)

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

(Ambient)

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



A Calculus of Bounded Capabilities

Thm: Subject Reduction

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



A Calculus of Bounded Capabilities

Thm: Subject Reduction

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

The missing bit:

Grave interferences in the use of spaces

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

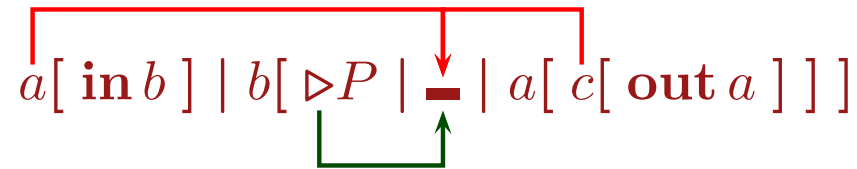
A Calculus of Bounded Capabilities

Thm: Subject Reduction

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

The missing bit:

Grave interferences in the use of spaces



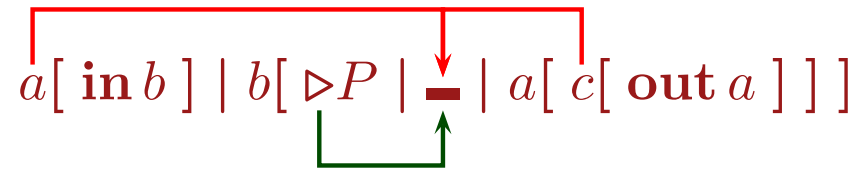
A Calculus of Bounded Capabilities

Thm: Subject Reduction

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

The missing bit:

Grave interferences in the use of spaces



$$\text{rec}(X^k)P \triangleq (\nu X^k)(!\text{opn } X . \triangleright^k \hat{P} \mid X[_{}^k])$$

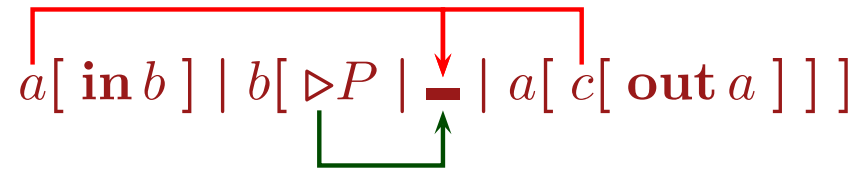
A Calculus of Bounded Capabilities

Thm: Subject Reduction

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

The missing bit:

Grave interferences in the use of spaces



$$\text{rec}(X^k)P \triangleq (\nu X^k)(! \text{opn } X . \triangleright^k \hat{P} \mid X[_{}^k])$$

$$\searrow (\nu X^k)(! \text{opn } X . \triangleright^k \hat{P} \mid \text{opn } X . \triangleright^k \hat{P} \mid X[_{}^k])$$

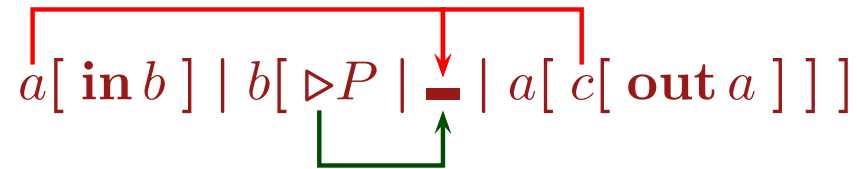
A Calculus of Bounded Capabilities

Thm: Subject Reduction

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

The missing bit:

Grave interferences in the use of spaces



$$\text{rec}(X^k)P \triangleq (\nu X^k)(! \text{opn } X . \triangleright^k \hat{P} \mid X[\underline{\quad}^k])$$

$$\searrow (\nu X^k)(! \text{opn } X . \triangleright^k \hat{P} \mid \text{opn } X . \triangleright^k \hat{P} \mid X[\underline{\quad}^k])$$

$$\searrow (\nu X^k)(! \text{opn } X . \triangleright^k \hat{P} \mid \triangleright^k \hat{P} \mid \underline{\quad}^k)$$

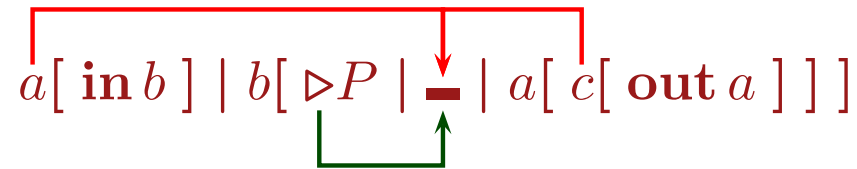
A Calculus of Bounded Capabilities

Thm: Subject Reduction

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

The missing bit:

Grave interferences in the use of spaces



$$\text{rec}(X^k)P \triangleq (\nu X^k)(! \text{opn } X . \triangleright^k \hat{P} \mid X[\underline{\quad}^k])$$

$$\searrow (\nu X^k)(! \text{opn } X . \triangleright^k \hat{P} \mid \text{opn } X . \triangleright^k \hat{P} \mid X[\underline{\quad}^k])$$

$$\searrow (\nu X^k)(! \text{opn } X . \triangleright^k \hat{P} \mid \triangleright^k \hat{P}) \mid \underline{\quad}^k \quad \text{Oooops}$$

Control Space Usage: Named Slots

$P ::= _a \mid a \triangleright^k P \mid \dots$ (spawn) $a \triangleright^k P \mid _a^k \searrow P$

Control Space Usage: Named Slots

$$P ::= _a \mid a \triangleright^k P \mid \dots \quad (\text{spawn}) \quad a \triangleright^k P \mid _a^k \searrow P$$

Example: Renaming slots

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

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

Control Space Usage: Named Slots

$$P ::= _a^k \mid a \triangleright^k P \mid \dots \quad (\text{spawn}) \quad a \triangleright^k P \mid _a^k \searrow P$$

Example: Renaming slots

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

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

Example: Recursion (now right):

$$\text{rec}(X^k)P \triangleq (\nu X)(!X \triangleright^k \hat{P} \mid _X^k), \quad \text{where } \hat{P} \triangleq P\{_X^k/X\}$$

Control Space Usage: Named Slots

$$P ::= _a \mid a \triangleright^k P \mid \dots \quad (\text{spawn}) \quad a \triangleright^k P \mid _a^k \searrow P$$

Example: Renaming slots

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

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

Example: Recursion (now right):

$$\text{rec}(X^k)P \triangleq (\nu X)(!X \triangleright^k \hat{P} \mid _X^k), \quad \text{where } \hat{P} \triangleq P\{_X^k/X\}$$

Example: Deriving Named Slots

$$_a \triangleq a[\ll \mid _]$$

$$a \triangleright^k P \triangleq (\nu n)(n[a^k \gg \cdot \triangleright^k \overline{\text{opn}} \cdot P] \mid \text{opn } n)$$



Conclusions

Typed Barbed Congruence:

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

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

This is sufficient to capture important differences.

Labelled Transition System: Easy enough.



Conclusions

Typed Barbed Congruence:

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

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 $B0C\alpha$; Equational theory; Smarter types; ...
- In general: A lot to be done. ...