

Equational Properties of Mobile Ambients

Andy Gordon, Microsoft Research

Joint work with Luca Cardelli, Microsoft Research

FoSSaCS'99, Amsterdam

Orientation: Ambients

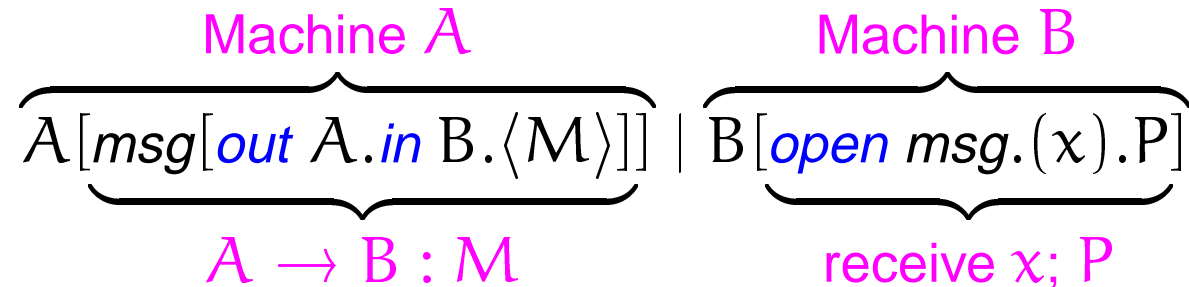
An ambient is a named, bounded place where computation happens; it is both a unit of mobility and a security perimeter.

A capability represents a right to move into or out of an ambient, or to dissolve its boundary.

Ambient security rests on the controlled distribution of capabilities; the right to enter an ambient does not imply the right to exit it.

One goal of this work is to develop a flexible, precise, secure, and typeful programming model for mobile software components.

Mobile Ambients: a packet from A to B



- Ambients may model both machines and packets
- Ambients are mobile: $\text{msg}[\dots]$ moves out of A and into B
- You need capability $\text{out } A$ to exit A ; capability $\text{in } B$ to enter B ; and capability open msg to dissolve msg
- There is an ether local to each ambient for message exchange

Ambient Behaviour, By Example

There are four basic reduction rules in the calculus:

$$\begin{aligned} & A[msg[*out* A.in B.\langle M \rangle]] \mid B[open\ msg.(x).P] \\ & \rightarrow A[] \mid msg[*in* B.\langle M \rangle] \mid B[open\ msg.(x).P] \\ & \rightarrow A[] \mid B[msg[\langle M \rangle] \mid open\ msg.(x).P] \\ & \rightarrow A[] \mid B[\langle M \rangle \mid (x).P] \\ & \rightarrow A[] \mid B[P\{x \leftarrow M\}] \end{aligned}$$

Definition: Contextual Equivalence (aka May Testing)

A standard semantic equivalence: $P \simeq Q$ iff the observable behaviour of an assembly with component P is unaffected by replacing P with Q . Example: quicksort \simeq bubble sort.

In the ambient calculus:

- Let $P \Downarrow n$ mean that process P may evolve in a series of steps to a process P' that has a top-level ambient named n .
- Let a **context** $\mathcal{C}()$ be a process with a hole; examples: just a hole $()$, down one level $n[()]$, guarded *in* $n.()$, replicated $!()$
- Let $P \simeq Q$ iff for all $n, \mathcal{C}()$, $\mathcal{C}(P) \Downarrow n \Leftrightarrow \mathcal{C}(Q) \Downarrow n$.

Example 1: Some Basic Equations

Some easy inequivalences:

- $p[]$ and $q[]$ distinguished by $()$
- $\text{open } p.0$ and $\text{open } q.0$ distinguished by $p[n[]] \mid ()$
- $\text{in } p.0$ and $\text{out } p.0$ distinguished by $m[n[()] \mid \text{out } p.\text{out } m] \mid p[]$

As in most process calculi, reduction does not imply equivalence:

- $n[] \mid \text{open } n.0 \rightarrow 0$ but $n[] \mid \text{open } n.0 \not\approx 0$

A law: for all P , $(\nu n)(n[] \mid \text{open } n.P) \simeq (\nu n)P$.

Example 2: Perfect Firewalls, Perfect Encryption

If nobody inside or outside an ambient knows its name, then it forms a perfect boundary between its inside and outside.

An ambient $n[P]$ abstractly models an internet firewall named n , enclosing a group of machines P .

The Perfect Firewall Equation: if $n \notin fn(P)$, then $(\nu n)n[P] \simeq \mathbf{0}$.

An ambient $k[\langle M \rangle]$ abstractly models a ciphertext $\{M\}_k$, obtained by encrypting a plaintext M with a key k .

The Perfect Encryption Equation: $(\nu k)k[\langle M \rangle] \simeq (\nu k)k[\langle M' \rangle]$
for all M, M' (compare $(\nu k)\bar{c}\langle\{M\}_k\rangle \simeq (\nu k)\bar{c}\langle\{M'\}_k\rangle$ from spi)

Example 3: Piloting an Agent Across a Firewall

Pre-arranged passwords k, k', k'' allow an agent to cross a firewall:

$$\mathit{Firewall} \triangleq (\nu w)w[k[\mathit{out} w.\mathit{in} k'.\mathit{in} w] \mid \mathit{open} k'.\mathit{open} k''.P]$$

$$\mathit{Agent} \triangleq k'[\mathit{open} k.k''[C]]$$

Assuming k, k', k'' do not occur in C or P , and w does not occur in C , we get the safety property:

$$(\nu k k' k'')(\mathit{Agent} \mid \mathit{Firewall}) \simeq (\nu w)w[C \mid P]$$

Problem 1: Chemical Soups

Structural congruence (Berry & Boudol, Milner) allows for:

- rearrangement: $P \mid (\nu n)Q \equiv (\nu n)(P \mid Q)$ if n not free in P, \dots
- garbage collection: $P \mid \mathbf{0} \equiv P, \dots$
- replication: $!P \equiv P \mid !P, !\mathbf{0} \equiv \mathbf{0}, \dots$

Reduction based on rule $P \equiv P', P' \rightarrow Q', Q' \equiv Q \Rightarrow P \rightarrow Q$.

This is great for many purposes!

Obeying page limits, calculating reductions, validating type systems, ...

But it's dreadful for others.

Try proving that if $\mathcal{C}(\mathbf{0}) \Downarrow n$ then $\mathcal{C}(P) \Downarrow n$.

Solution: Hardenings and Labelled Transitions

A **concretion** is a phrase $(\nu \vec{p}) \langle P' \rangle P''$ (Milner).

New idea: a **hardening** $P > (\nu \vec{p}) \langle P' \rangle P''$ identifies a top-level process P' of P , the residue P'' , and the bindings \vec{p} they share.

For example, $n[p \square] \mid \text{open } n.0$ has two hardenings:

$$n[p \square] \mid \text{open } n.0 > (\nu) \langle n[p \square] \rangle (0 \mid \text{open } n.0)$$

$$n[p \square] \mid \text{open } n.0 > (\nu) \langle \text{open } n.0 \rangle (n[p \square] \mid 0)$$

Definition of Hardening

Hardening: $P > (\nu \vec{p}) \langle P' \rangle P''$

$M \in \{in\ n, out\ n, open\ n\}$

$M.P > (\nu) \langle M.P \rangle \mathbf{0}$

$n[P] > (\nu) \langle n[P] \rangle \mathbf{0}$

$P > (\nu \vec{p}) \langle P' \rangle P'' \quad \{\vec{p}\} \cap fn(Q) = \emptyset$

$P \mid Q > (\nu \vec{p}) \langle P' \rangle (P'' \mid Q)$

$P > (\nu \vec{p}) \langle P' \rangle P''$

$(\nu n)P > \overline{(\nu n)} (\nu \vec{p}) \langle P' \rangle P''$

$Q > (\nu \vec{q}) \langle Q' \rangle Q'' \quad \{\vec{q}\} \cap fn(P) = \emptyset$

$P \mid Q > (\nu \vec{q}) \langle Q' \rangle (P \mid Q'')$

$P > (\nu \vec{p}) \langle P' \rangle P''$

$!P > (\nu \vec{p}) \langle P' \rangle (P'' \mid !P)$

Definition of Labelled Transitions

First, a transition $P \xrightarrow{M} P'$, for $M \in \{in\ n, out\ n, open\ n\}$, means that P has effect M on parent or sibling n , and evolves to P' .

M-transitions: $P \xrightarrow{M} P'$ where $M \in \{in\ n, out\ n, open\ n\}$

$$\frac{P > (\nu \vec{p}) \langle M.P' \rangle P'' \quad fn(M) \cap \{\vec{p}\} = \emptyset}{P \xrightarrow{M} (\nu \vec{p}) (P' \mid P'')}$$

For example:
$$\frac{out\ A.in\ B.\langle M \rangle > (\nu) \langle out\ A.in\ B.\langle M \rangle \rangle \mathbf{0}}{out\ A.in\ B.\langle M \rangle \xrightarrow{out\ A} in\ B.\langle M \rangle \mid \mathbf{0}}$$

Second, a transition $P \xrightarrow{\tau} P'$ means that P internally evolves in one step to P' . Here is the rule for exiting an ambient:

τ -transitions: $P \xrightarrow{\tau} P'$

$$\frac{P > (\nu \vec{p}) \langle n[Q] \rangle P' \quad Q > (\nu \vec{q}) \langle m[R] \rangle Q' \quad R \xrightarrow{\text{out } n} R' \quad n \notin \{\vec{q}\}}{P \xrightarrow{\tau} (\nu \vec{p}) ((\nu \vec{q}) (m[R'] \mid n[Q']) \mid P')}$$

For example:

$$A[msg[out A.in B.\langle M \rangle]] \xrightarrow{\tau} msg[in B.\langle M \rangle \mid \mathbf{0}] \mid A[\mathbf{0}] \mid \mathbf{0}$$

Theorems about Hardening and Labelled Transitions

- (1) If $P > (\nu \vec{p}) \langle P' \rangle P''$ then $P \equiv (\nu \vec{p}) (P' \mid P'')$.
- (2) If $P \equiv Q$ and $Q > (\nu \vec{r}) \langle Q' \rangle Q''$ then there are P' and P'' with $P > (\nu \vec{r}) \langle P' \rangle P''$, $P' \equiv Q'$, and $P'' \equiv Q''$.
- (3) $P \rightarrow Q$ if and only if $P \xrightarrow{\tau} \equiv Q$.
- (4) $P \Downarrow n$ if and only if there are Q, \vec{q}, Q', Q'' such that $P \xrightarrow{\tau}^* Q$, $Q > (\nu \vec{q}) \langle n[Q'] \rangle Q''$, and $n \notin \{\vec{q}\}$.

Hence, we solve the problem of proving $\mathcal{C}(\mathbf{0}) \Downarrow n$ implies $\mathcal{C}(P) \Downarrow n$.

Problem 2: The Trouble with Contexts

General contexts $\mathcal{C}()$ possess neither of the desirable properties:

- (1) they have a unique hole, preserved by reduction,
- (2) they are identified up to alpha-conversion.

Usual solution: identify a limited set of contexts satisfying (1), (2), and:

- (3) **A Context Lemma:** $P \simeq Q$ if and only if for all limited contexts H and names n , that $H\{P\} \Downarrow n \Leftrightarrow H\{Q\} \Downarrow n$.

In CCS and the π -calculus, the limited contexts are simply parallel observers; $H ::= - \mid R$. (De Nicola and Hennessy)

Parallel Observers and the Ambient Calculus

Let $P = \text{out } p.0$ and $Q = 0$.

- We have $P \mid R \Downarrow n \Leftrightarrow Q \mid R \Downarrow n$ for all n and R ,
- while if $\mathcal{C}() = p[m[()]]$ we have $\mathcal{C}(P) \Downarrow m$ but not $\mathcal{C}(Q) \Downarrow m$.

Therefore the set of parallel observers does not satisfy a context lemma in the ambient calculus.

Solution: Harnesses

Our solution is to augment parallel observers with ambients:

Harnesses:

$H ::=$	harnesses
$-$	unique hole
$(\nu n)H$	restriction
$P \mid H$	left composition
$H \mid Q$	right composition
$n[H]$	ambient

We identify harnesses up to alpha-conversion

If $H = (\nu n)-$, its instantiation $H\{n[]\}$ is $(\nu n')n[]$

By a careful analysis, we have proved that harnesses satisfy the desired context lemma.

Problem 3: How Do We Analyse $H\{P\} \rightarrow R$?

In lots of proofs that appeal to our context lemma, we have the problem of analysing reductions like $H\{P\} \rightarrow R$.

Intuitively, either P or H evolves on its own, or they interact.

The best formalisation we have found of this is:

An Activity Lemma: $H\{P\} \rightarrow R$ if and only if:

(Act Proc) $P \rightarrow P'$ with $R \equiv H\{P'\}$, or

(Act Har) $H \rightarrow H'$ with $R \equiv H'\{P\}$, or

(Act Inter) $H \bullet P \rightsquigarrow R$.

Let $H \bullet P \rightsquigarrow R$ if and only if there are H' and \vec{r} with $\{\vec{r}\} \cap \text{fn}(P) = \emptyset$, and one of the following holds:

(Inter In) $H \equiv (\nu \vec{r})H'\{m[- \mid R'] \mid n[R'']\}$, $P \xrightarrow{\text{in } n} P'$,
and $R \equiv (\nu \vec{r})H'\{n[m[P' \mid R'] \mid R'']\}$

(Inter Out) $H \equiv (\nu \vec{r})H'\{n[m[- \mid R'] \mid R'']\}$, $P \xrightarrow{\text{out } n} P'$,
and $R \equiv (\nu \vec{r})H'\{m[P' \mid R'] \mid n[R'']\}$

(Inter Open) $H \equiv (\nu \vec{r})H'\{- \mid n[R']\}$, $P \xrightarrow{\text{open } n} P'$,
and $R \equiv (\nu \vec{r})H'\{P' \mid R'\}$

(Inter Amb) $P > (\nu \vec{p})\langle n[Q] \rangle P'$ and one of the following holds:

(1) $Q \xrightarrow{\text{in } m} Q'$, $H \equiv (\nu \vec{r})H'\{- \mid m[R']\}$, $\{\vec{p}\} \cap \text{fn}(m[R']) = \emptyset$,
and $R \equiv (\nu \vec{r})H'\{(\nu \vec{p})(P' \mid m[n[Q'] \mid R'])\}$

(2) $Q \xrightarrow{\text{out } m} Q'$, $H \equiv (\nu \vec{r})H'\{m[- \mid R']\}$, $m \notin \{\vec{p}\}$,
and $R \equiv (\nu \vec{r})H'\{(\nu \vec{p})(n[Q'] \mid m[P' \mid R'])\}$

(3) $H \equiv (\nu \vec{r})H'\{m[R' \mid \text{in } n.R''] \mid -\}$, $\{\vec{p}\} \cap \text{fn}(m[R' \mid \text{in } n.R'']) = \emptyset$,
and $R \equiv (\nu \vec{r})H'\{(\nu \vec{p})(n[Q \mid m[R' \mid R'']] \mid P')\}$

(4) $H \equiv (\nu \vec{r})H'\{- \mid \text{open } n.R'\}$, $n \notin \{\vec{p}\}$,
and $R \equiv (\nu \vec{r})H'\{(\nu \vec{p})(Q \mid P') \mid R'\}$

Summary: Difficulty of Deriving Ambient Equations

Problem 1: Reduction defined using structural congruence

Solution: use $P > (\nu \vec{p}) \langle P' \rangle P''$ and $P \xrightarrow{\tau} P'$ instead

$$\text{Thm 1: } P \rightarrow Q \Leftrightarrow P \xrightarrow{\tau} \equiv Q$$

Problem 2: Equivalence defined using arbitrary contexts

Solution: **Thm 2:** $P \simeq Q$ iff for all H, n , $H\{P\} \Downarrow n \Leftrightarrow H\{Q\} \Downarrow n$

Problem 3: How to analyse reductions of a process in harness

Solution: **Thm 3:** $H\{P\} \rightarrow R$ iff (1) $P \rightarrow P'$ and $R \equiv H\{P'\}$, or

(2) $H \rightarrow H'$ and $R \equiv H'\{P\}$, or

(3) $H \bullet P \rightsquigarrow R$

Examples: Perfect firewall and cipher equations; firewall crossing.

Assessment

- We wanted to prove equations asserting simple security properties of ambients, and we succeeded. But:
- Reasoning about higher-order hierarchical processes is difficult: Castagna and Vitek faced similar difficulties with their Seal calculus
Is there an alternative to operational semantics?
- Defining reduction from structural congruence is a mixed blessing.
The laws $P \mid \mathbf{0} \equiv P$ and $!\mathbf{0} \equiv \mathbf{0}$ are not so innocent!
- Defining labelled transitions from hardening works well.
- Activity lemma is useful but suspicious:
Is there a less monolithic definition?