A G-Local Pi Calculus

Chiara Bodei, Dung Dinh, and GianLuigi Ferrari

University of Pisa

April 2, 2011
Content

- Motivations
- Syntax and Semantics
- An example
- Control Flow Analysis
- Future Works
Motivations

applications

\( \text{req } r_3 \)

\( P_1 \)

\( P_2 \)

\( P_3 \)

\( Q_1 \)

\( \text{req } r_4 \)

resources

\( r_4 \)

\( r_3 \)

\( r_2 \)

\( r_1 \)
Motivations

applications

resources

req r₃

P₁ P₂ P₃

Q₁

r₁ r₂ r₃ r₄
Motivations

- A formal model for modern distributed systems
Motivations

- A formal model for modern distributed systems
  - Resource awareness: mechanisms to express and enforce policies governing resource usages
Motivations

▶ A formal model for modern distributed systems
  ▶ Resource awareness: mechanisms to express and enforce policies governing resource usages
  ▶ Reasoning techniques: static and dynamic checks of the program behavior

A G-Local Pi Calculus University of Pisa
A Process Calculus Approach

G-Local $\pi$-Calculus:
- processes as loosely couple entities with
  - primitives based on $\pi$-calculus
  - primitives to acquire and discharge resources
- resources as stateful entities with
  - local state + global properties
Representing resources

A triple of

- $r$: a resource name
- $\varphi$: a policy
  - $\varphi$ is specified by resource-aware logics
- $\eta$: a state
  - logs
Resource management

Two primitives for managing resource boundaries:

- a resource joint point: \((r, \varphi, \eta)\{Q\}\)
  - an action prefix: \(\alpha(r; p).Q\)

- a resource request point: \(\text{req}(r)\{Q\}\)

- Note that \(Q\) is a sequential process
Semantics - Samples

- Available resources: \((r, \varphi, \epsilon)\{0\}\)

- A structural rule of resource movement:
  \[(r_1, \varphi_1, \eta_1)\{(r_2, \varphi_2, \eta_2)\{0\} \parallel Q\} \equiv (r_2, \varphi_2, \eta_2)\{0\} \parallel (r_1, \varphi_1, \eta_1)\{Q\}\]

- this rule simulates reconfigurations of resources
Semantics - Samples

- Resource Usages:

\[
\begin{align*}
Q & \xrightarrow{\alpha(r;p)} Q' \\
& \quad \text{check}(\eta.\alpha(r;p), \varphi) \\
(r, \varphi, \eta)\{Q\} & \xrightarrow{\tau} (r, \varphi, \eta.\alpha(r;p))\{Q'\}
\end{align*}
\]

- \(\eta' = \eta.\alpha(r;p):\) an updated state
- predicate \(\text{check}(\eta, \varphi)\) checks validity of \(\varphi\) on \(\eta\)
Semantics - Samples

Resource acquisition:

\[
\text{req}(r)\{Q\} \parallel (r, \varphi, \eta)\{0\} \xrightarrow{\tau} (r, \varphi, \eta)\{Q\}
\]
Semantics - Samples

Resource release:

\[
Q \neq 0 \land r \notin \text{@Res}(Q) \\
(r, \varphi, \eta)\{Q\} \xrightarrow{\tau} (r, \varphi, \eta)\{0\} \parallel Q
\]

- \( r \notin \text{@Res}(Q) \): \( r \) - not “in use” in \( Q \)
- \( Q \neq 0 \): avoid loops
An example - a robot scenario
An example - cont.

A simple model:

\[ R_1 = \text{req}(\text{item})\{ \text{East}(\text{item}).0 \} \]
\[ R_2 = \text{req}(\text{item})\{ \text{East}(\text{item}).0 \} \]
\[ R'_2 = \text{req}(\text{item})\{ \text{North}(\text{item}).0 \} \]
\[ R_3 = \text{req}(\text{item})\{ \text{North}(\text{item}).0 \} \]

\[ S = (\text{item}, \varphi, \epsilon)\{ 0 \} \parallel R_1 \parallel R_2 \parallel R'_2 \parallel R_3 \]

the policy \( \varphi \) constrains movement of the item on the grid.
Control Flow Analysis (CFA)

- CFA represents an abstraction of the actual executions
- Concretisation cannot be precise

Static
- Event E is included
- Event E is not included

Dynamic
- Event E can happen
- Event E never happens
Control Flow Analysis - cont.

What are abstractions of behaviour?

- $\rho$ - name bindings:
  - $a \in \rho(x)$: $a$ can be bound to $x$

- $\kappa$ - values sent on each channel:
  - $a \in \kappa(x)$: $a$ can be sent on $x$

- $\Gamma$ - resource behaviour:
  - $(\phi, \eta) \in \Gamma(r)$ then $\eta$ - a possible trace over $r$, respecting $\phi$

- $\psi$ - errors:
  - $(\phi, \eta) \in \psi(r)$, then $\eta$ - a violating possible trace over $r$
Control Flow Analysis - cont.

- Judgment of analysis: \((\rho, \kappa, \Gamma, \psi) \models^\delta P\)
- **Subject Reduction**: \((\rho, \kappa, \Gamma, \psi) \models^\delta P\) and \(P \xrightarrow{\tau}^* P'\), then \((\rho, \kappa, \Gamma, \psi) \models^\delta P'\).
- **Existence of solutions** \((\rho, \kappa, \Gamma, \psi)\): there always exists a least solution
CFA with the robot scenario

- with annotations:

\[
\begin{align*}
R_1 &= \text{req}(\text{item})\{ \text{East}(\text{item}).0 \}^{\chi_1} \\
R_2 &= \text{req}(\text{item})\{ \text{East}(\text{item}).0 \}^{\chi_2} \\
R'_2 &= \text{req}(\text{item})\{ \text{North}(\text{item}).0 \}^{\chi'_2} \\
R_3 &= \text{req}(\text{item})\{ \text{North}(\text{item}).0 \}^{\chi_3} \\
\end{align*}
\]

\[
S = (\text{item}, \varphi, \epsilon)\{ 0 \}^{\chi_0} \parallel R_1 \parallel R_2 \parallel R'_2 \parallel R_3
\]

- CFA result on trajectories of \textit{item}:

\begin{itemize}
  \item (\textit{East(item)}.\textit{North(item)}, \chi_0.\chi_1.\chi_2')
    \begin{itemize}
      \item this is a bad trajectory!
    \end{itemize}
  \item (\textit{East(item)}.\textit{East(item)}.\textit{North(item)}, \chi_0.\chi_1.\chi_2.\chi_3)
    \begin{itemize}
      \item this is a trajectory leading to the required location
    \end{itemize}
\end{itemize}
Future Works

- Investigate logics for specifying policies
  - Focus on decidability

- Link mobility: communication mechanisms of resource names
  - Bound resource names and the predicate @Res

- Behavioral types for the full calculus
  - Model checking of behavioral types

- More effective views of resources
  - Resource movement
  - Exponential availability
Q & A

Thank you!

and questions?
Future Works

- more effective views of resources:
  
  - resource disappearance:
    
    $$(r, \varphi, \eta)\{0\} \xrightarrow{\tau} 0$$
Future Works

- more effective views of resources:
  - resource appearance:

\[ P \xrightarrow{\tau} P \parallel (r, \varphi, \eta)\{0\} \]
Future Works

- more effective views of resources:
  - resource coordination: restrict resource movement

\[
(r_1, \varphi_1, \eta_1) \{(r_2, \varphi_2, \eta_2)\{0\} \parallel Q\} \\
\equiv (r_2, \varphi_2, \eta_2)\{0\} \parallel (r_1, \varphi_1, \eta_1)\{Q\}
\]
Future Works

- more effective views of resources:
  - resource coordination: restrict resource movement

\[
(r_1, \varphi_1, \eta_1) \{ (r_2, \varphi_2, \eta_2) \{ 0 \} \parallel Q \}
\equiv (r_2, \varphi_2, \eta_2) \{ 0 \} \parallel (r_1, \varphi_1, \eta_1) \{ Q \}
\]
Future Works

- more effective views of resources:
  - exponential availability of resources:

\[ !(r, \varphi, \eta) \equiv !(r, \varphi, \eta) \parallel (r, \varphi, \eta) \]
Future Works

- more effective views of resources:
  - exponential availability of resources:
    \[ !(r, \varphi, \eta) \equiv !(r, \varphi, \eta) \parallel (r, \varphi, \eta) \]