An Introduction to the π-Calculus

Graduate seminar "Safe and secure cognitive systems"

Bremen, 27.01.2006

Overview

- Comparison of the basic concepts of CCS, the value passing calculus and the π-calculus.
- LTS-semantics of the π-calculus (commitment).
- Notions of behavioral equivalence for the π-calculus.

Syntax

Finite indexing set I, set of channels C, set of values V and a set of variables Var.

- CCS: $P ::= \Sigma_{i \in I} \alpha_i.P_i \mid P|Q \mid (\nu x)P \mid !P$
- VPC: $P ::= \Sigma_{i \in I} \beta_i.P_i \mid P|Q \mid (\nu x)P \mid !P$
- Π: $P ::= \Sigma_{i \in I} \pi_i.P_i \mid P|Q \mid (\nu x)P \mid !P$

$\alpha_i \in \{\overline{a} \mid a \in C\} \cup C$.

$\beta_i \in \{a(x) \mid a \in C, x \in Var\} \cup \{\overline{a}(y) \mid a \in C, y \in V \cup Var\}$.

$\pi_i \in \{a(x) \mid a, x \in C \cup Var\} \cup \{\overline{a}(y) \mid a, y \in C \cup Var\}$.

Structural congruence

$\equiv_{CCS}$, $\equiv_{VPC}$ and $\equiv_{\Pi}$ are respectively the smallest congruences adhering to:

- Identification of alpha-equivalent processes (bound names).
- $(\mathcal{N}_{\mathcal{PA}}/\equiv_{\mathcal{PA}}, +, \mathbf{0})$ is a symmetric monoid.
- $(\mathcal{PA}/\equiv_{\mathcal{PA}}, |, \mathbf{0})$ is a symmetric monoid.
- $!P \equiv_{\mathcal{PA}} P \mid !P$
- $(\nu x)\mathbf{0} \equiv_{\mathcal{PA}} \mathbf{0}$, $(\nu x)(\nu y)P \equiv_{\mathcal{PA}} (\nu y)(\nu x)P$,
  if $x \notin fn(P)$ then $(\nu x)(P \mid Q) \equiv_{\mathcal{PA}} P \mid (\nu x)Q$.

Semantics

Central reduction rules:

- CCS: $(\ldots + a.P) \mid (\ldots + \overline{a}.Q) \longrightarrow_{CCS} P \mid Q$
- VPC: $(\ldots + a(y).P) \mid (\ldots + \overline{a}(x).Q) \longrightarrow_{VPC} P\{x/y\} \mid Q$
- Π: $(\ldots + a(y).P) \mid (\ldots + \overline{a}(x).Q) \longrightarrow_{\Pi} P\{x/y\} \mid Q$

Additional standard rules:

- $P \longrightarrow_{\mathcal{PA}} P'$ implies $P \mid Q \longrightarrow_{\mathcal{PA}} P' \mid Q$.
- $P \longrightarrow_{\mathcal{PA}} P'$ implies $(\nu x)P \longrightarrow_{\mathcal{PA}} (\nu x)P'$.
- $Q \equiv_{\mathcal{PA}} P$, $P \longrightarrow_{\mathcal{PA}} P'$ and $P' \equiv_{\mathcal{PA}} Q'$ imply $Q \longrightarrow_{\mathcal{PA}} Q'$.

Some simple examples

CCS:

- $!a.\overline{b}.\mathbf{0} \mid !\overline{a}.b.\mathbf{0} \equiv_{CCS} a.\overline{b}.\mathbf{0} \mid \overline{a}.b.\mathbf{0} \mid !a.\overline{b}.\mathbf{0} \mid !\overline{a}.b.\mathbf{0} \longrightarrow_{CCS}$
  $\overline{b}.\mathbf{0} \mid b.\mathbf{0} \mid !a.\overline{b}.\mathbf{0} \mid !\overline{a}.b.\mathbf{0} \longrightarrow_{CCS}$
  $\mathbf{0} \mid \mathbf{0} \mid !a.\overline{b}.\mathbf{0} \mid !\overline{a}.b.\mathbf{0} \equiv_{CCS} !a.\overline{b}.\mathbf{0} \mid !\overline{a}.b.\mathbf{0}$

VPC:

- $\overline{a}(5).b(x).\overline{c}(x).\mathbf{0} \mid a(y).\overline{b}(y).\mathbf{0} \mid c(z).\overline{d}(z) \longrightarrow_{VPC}$
  $b(x).\overline{c}(x).\mathbf{0} \mid \overline{b}(5).\mathbf{0} \mid c(z).\overline{d}(z) \longrightarrow_{VPC}$
  $\overline{c}(5).\mathbf{0} \mid \mathbf{0} \mid c(z).\overline{d}(z) \equiv_{VPC} \overline{c}(5).\mathbf{0} \mid c(z).\overline{d}(z) \longrightarrow_{VPC}$
  $\mathbf{0} \mid \overline{d}(5) \equiv_{VPC} \overline{d}(5)$

Π:

- $\overline{a}(b).a(x).\overline{x}(x) \mid a(y).\overline{y}(a) \mid b(z).\overline{z}(c) \longrightarrow_{\Pi}$
  $a(x).\overline{x}(x) \mid \overline{b}(a) \mid b(z).\overline{z}(c) \longrightarrow_{\Pi}$
  $a(x).\overline{x}(x) \mid \overline{a}(c) \longrightarrow_{\Pi}$
  $\overline{c}(c)$

Early LTS Semantics

$$\frac{P \xrightarrow{au}_E P' \quad Q \xrightarrow{\overline{a}u}_E Q'}{P \mid Q \xrightarrow{\tau}_E P' \mid Q'}$$

$$\frac{}{\overline{a}(u).P \xrightarrow{\overline{a}u}_E P} \qquad \frac{}{a(x).P \xrightarrow{au}_E P\{u/x\}}$$

$$\frac{P \xrightarrow{\alpha}_E P'}{P + Q \xrightarrow{\alpha}_E P'} \qquad \frac{P \xrightarrow{\alpha}_E P'}{P \mid Q \xrightarrow{\alpha}_E P' \mid Q} \qquad \frac{P \xrightarrow{\alpha}_E P' \quad fn(\alpha) \notin \{x, \overline{x}\}}{(\nu x)P \xrightarrow{\alpha}_E (\nu x)P'}$$

$$\frac{P \equiv P' \quad P \xrightarrow{\alpha}_E Q \quad Q \equiv Q'}{P' \xrightarrow{\alpha}_E Q'}$$

Result: $P \xrightarrow{\tau}_E Q$ iff $P \longrightarrow_\Pi Q$.

Early Bisimulation and congruence

- A (strong) early bisimulation is a symmetric relation ρ s.t. $P \rho Q$ implies
  - If $P \xrightarrow{\alpha}_E P'$ then $\exists Q'.Q \xrightarrow{\alpha}_E Q'$ and $P' \rho Q'$.
- The union $\dot{\sim}_E$ of all early bisimulations (called early bisimilarity) is not a congruence (is not preserved by input prefixing).
- Early congruence $\sim_E$ (defined as $P \sim_E Q$ if for all subsitutions σ, $P\sigma \mathrel{\dot{\sim}_E} Q\sigma$) is the largest congruence contained in early bisimilarity.

Late LTS semantics

Change $\dfrac{}{a(x).P \xrightarrow{au}_E P\{u/x\}}$ to $\dfrac{}{a(x).P \xrightarrow{\underline{a}x}_L P}$ and

change $\dfrac{P \xrightarrow{au}_E P' \quad Q \xrightarrow{\overline{a}u}_E Q'}{P \mid Q \xrightarrow{\tau}_E P' \mid Q'}$ to $\dfrac{P \xrightarrow{\underline{a}x}_L P' \quad Q \xrightarrow{\overline{a}u}_L Q'}{P \mid Q \xrightarrow{\tau}_L P'\{u/x\} \mid Q'}$.

- $P \xrightarrow{\underline{a}x}_L Q$ means "P inputs something to replace x in Q",
- $P \xrightarrow{ax}_E Q$ means "P receives x and continues as Q".

Result: $P \xrightarrow{\tau}_L Q$ iff $P \xrightarrow{\tau}_E Q$ iff $P \longrightarrow_\Pi Q$.

Late Bisimulation and congruence

- A (strong) late bisimulation is a symmetric relation ρ s.t. $P\rho Q$ implies
  - If $P \xrightarrow{a x}_L P'$ then $\exists Q'.Q \xrightarrow{a x}_L Q'$ and $\forall u.P'\{u/x\}\rho Q'\{u/x\}$.
  - If $P \xrightarrow{\alpha}_E P'$ then $\exists Q'.Q \xrightarrow{\alpha}_E Q'$ and $P'\rho Q'$.
- Late bisimilarity $\dot{\sim}_L$ is again not a congruence.
- Late congruence $\sim_L$ (defined as $P \sim_L Q$ if for all subsitutions σ, $P\sigma \dot{\sim}_L Q\sigma$) is the largest congruence contained in late bisimilarity.

Result: $\sim_L \subset \sim_E$.

Barbed congruence

- A process Q occurs unguarded in P if it occurs in P but not under a prefix.
- For a name n, the communication subject $x \in \{n, \overline{n}\}$ is observable at process P (denoted by $P \downarrow x$) if $x(z).Q$ occurs unguarded in P for some z and if n is not restricted.
- A barbed bisimulation is a symmetric ρ s.t. $P \rho Q$ implies
  (a) If $P \longrightarrow_{\Pi} P'$ then $\exists Q'.Q \longrightarrow_{\Pi} Q'$ and $P' \rho Q'$.
  (b) If $P \downarrow n$ then $Q \downarrow n$.

Barbed Congruence ctd.

- Contexts $\mathcal{C}$ are processes with exactly one hole.
- Barbed congruence $\sim_B$ is the largest congruence contained in barbed bisimilarity: For a barbed bisimulation $\dot{\sim}_B$ and all contexts $\mathcal{C}$,

  $P \sim_B Q$ if $\mathcal{C}[P] \dot{\sim}_B \mathcal{C}[Q]$.
- Important result: $\sim_B = \sim_E$.

Abstractions, Concretions

- An abstraction F is of the form $(\lambda x)P$, a concretion C is of the form $[x]P$. Agents A are either an abstraction or a concretion.
- Extending restriction, parallel composition and structural congruence to agents ensures that every abstraction F has a standard form

  $F \equiv (\lambda x)P$

  and every concretion C has a standard form

  $C \equiv (\nu x)[x]P$ or $C \equiv [x]P$.

The Commitment relation

$$\frac{P \overset{a}{\succ} F \quad Q \overset{\overline{a}}{\succ} C}{P \mid Q \overset{\tau}{\succ} F \bullet C}$$

$$\frac{}{c.E \overset{c}{\succ} E} \qquad \frac{P \equiv P' \quad P \overset{c}{\succ} E \quad E \equiv E'}{P' \overset{c}{\succ} E'}$$

$$\frac{P \overset{c}{\succ} E}{P + Q \overset{c}{\succ} E} \qquad \frac{P \overset{c}{\succ} E}{P \mid Q \overset{c}{\succ} E \mid Q} \qquad \frac{P \overset{c}{\succ} E \quad c \notin \{x, \overline{x}\}}{(\nu x)P \overset{c}{\succ} (\nu x)E}$$

where for $F \equiv (\lambda y)P$ and $C \equiv (\nu x)[x]Q$, $F \bullet C \overset{def}{=} (\nu x)(P\{x/y\} \mid Q)$.

Result: $P \overset{\tau}{\succ} P'$ iff $P \longrightarrow_{\Pi} P'$.

The commitment congruence (largest congruence contained in commitment bisimulation) coincides to early congruence.

Conclusion

- From CCS to VPC to π-calculus. From synchronisation to communication of values to communication of links.
- Early, late and commitment semantics. Commitment semantics seems to be most elegant (especially for the polyadic π-calculus).
- Early and commitment congruences coincide to barbed congruence which is seen as the natural behavioral equivalence for the π-calculus.

Further topics: weak, open bisimulations; higher order, asynchronous π-calculi; symbolic transition semantics.