LCD (21/04)

* PI- CALCULUS

example : PIZZA PLACE

customer $C = \overline{askPizza} .\ pay .\ pizza .\ 0$

pizza place $P = askPizza .\ pay .\ \overline{pizza} .\ P$

CCS value passing

$C = \overline{askPizza}(calzone) .\ \overline{pay}(5€) .\ change(z) .\ (pizza(\omega) .\ \overline{eat}(\omega) .\ 0 +$
$fail . 0)$

$P = askPizza(x) .\ pay(y) .\ \text{if } (price(x) \leq y)$
$\text{then } \overline{change}(y - price(x)) .\ \overline{pizza}(x) .\ P$
$\text{else } \overline{change}(y) .\ \overline{fail} .\ P$

$(C \mid P) \setminus \{askPizza, pay, change, ---\} \quad \mid C$

$\wr$

$(0 \mid P) \setminus \{askPizza, pay, ---\} \quad \mid C$

PROBLEM : processes can communicate only on channels known and shared since the beginning, statically.

Example : Pizza place with home delivery.

channel

$C = \overline{askPizza}(home) .\ \overline{pay} .\ home(x) .\ \overline{eat}(x) .\ 0$

$P = askPizza(y) .\ pay .\ (\nu\, pizza)\ \overbrace{(\overline{y}\langle pizza\rangle .\ P)}^{(*)}$

nu
new

→ "pizza" is private to (*)
$(\ *\ ) \setminus pizza$

→ "pizza" is a new channel in (*)

$$C \mid P \xrightarrow{\tau} \overline{pay}.home(x).\overline{eat}(x).0 \mid pay.(\nu\, pizza)(\overline{home}\langle pizza\rangle.P)$$

$$\xrightarrow{\tau} home(x).\overline{eat}(x).0 \mid (\nu\, pizza)(\overline{home}\langle pizza\rangle.P)$$

$$\xrightarrow{?} (\nu\, pizza)(\overline{eat}(pizza).0 \mid P)$$

$$\xrightarrow{\overline{eat}(?)} (\nu\, pizza)(\underbrace{0 \mid P}_{\equiv\ P})$$

$$\equiv$$

$$(\nu\, pizza)(ask\,Pizza(y).pay.(\nu\, pizza)(\overline{y}\langle pizza\rangle.P))$$

$$\equiv$$

$$ask.Pizza(y).pay.(\nu\, pizza)(\overline{y}.(pizza).P) \equiv P$$

PI - CALCULUS $\equiv$ CCS + channel creation
channel passing

* Syntax

set of channels N x, y, z a, b, c

processes $P ::= S \mid P_1 \mid P_2 \mid (\nu x)\, P$

- create a channel x local to P
- x is private in P

$S ::= 0 \mid \pi.P \mid S_1 + S_2$

$\pi ::= x(z) \mid \overline{x}(z) \mid \tau \mid [x=y]\pi$

binder

complication

z used in P

$$x(z).\ P \qquad =_\alpha \qquad x(w).\ P\{^{w}/_{z}\}$$

$$(\nu x)\ P \qquad =_\alpha \qquad (\nu w)\ P\{^{w}/_{x}\}$$

α - equivalence

(w not used in P)

$$y(z).\ \bar{z}(x).0 \quad \neq_\alpha \quad y(x).\ \bar{z}(x).0$$

$$y(z).\ \bar{z}(x).0 \quad \{^{z}/_{x}\} \quad = \quad y(z).\ \bar{z}(z).0$$

$$\equiv_\alpha \ y(w).\ \bar{z}(w).0 \quad \{^{z}/_{x}\} \quad = \quad y(w).\ \bar{z}(w).0 \ \not\equiv_\alpha$$

⋮ capture free substitutions ....

Operational Rules

$$P \xrightarrow{\ \bigcirc\ } P'$$

$$\frac{}{a(x).P \xrightarrow{ab} P\{^{b}/_{x}\}}$$

capture free substitution

$$\frac{}{\bar{a}b.\ P \xrightarrow{\bar{a}b} P}$$

$$\frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q}$$

$$\frac{P \xrightarrow{\bar{a}b} P' \qquad Q \xrightarrow{ab} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'}$$

* Interacting on private names?

$$\frac{P \xrightarrow{\alpha} P'}{(\nu z)\, P \xrightarrow{?} ?}$$

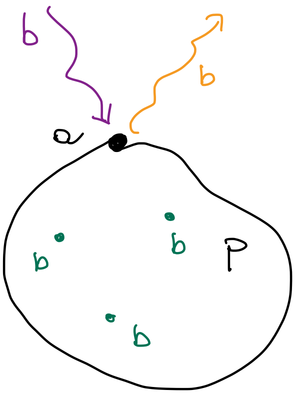
INPUT

$$\frac{P \xrightarrow{ab} P'}{(\nu z) P \xrightarrow{ab} (\nu z) P'} \quad ?$$

OUTPUT

$$\frac{P \xrightarrow{\bar{a}b} P'}{(\nu z)\ P \xrightarrow{\bar{a}b} (\nu z)\ P'} \quad ?$$

YES	$z \neq a, b$	YES
NO	$z = a$	NO
NO	$z \neq a$ $z = b$	



$$\frac{P \xrightarrow{\bar{a}b} P'}{(\nu b) P \xrightarrow{\bar{a}(\nu b)} P'} \qquad \text{(open)}$$

$$\frac{P \xrightarrow{\bar{a}(\nu b)} P' \qquad Q \xrightarrow{ab} Q'}{P \mid Q \xrightarrow{\tau} (\nu b)(P' \mid Q')} \qquad \text{(close)}$$

→ behavioural equivalence (weak , strong

early , late

⋮

→ logic (nominal logic) ∃ secret φ

∀ " .