Distinguishing between Communicating Transactions

Matthew Hennessy
Trinity College Dublin

joint work with Vasileois Koutavas, Maciej Gadza

OPTCS'17 Vienna, June 2017

Paper available at:
www.scss.tcd.ie/Matthew.Hennessy/onlinepubs.html

Outline

Explaining why ....

process descriptions denote different behaviours

General scenario:

$$P_1 \not\approx_{\text{behav}} P_2 \quad \text{iff} \quad P_2 \vdash \phi,\ P_2 \not\vdash \phi \qquad \text{for some property } \phi$$

Property ϕ explains why P_1, P_2 behave differently

Counterexample synthesis: automatic

Concurrency workbench MCRL2 UPPAAL . . .

Explaining why ....

process descriptions denote different behaviours

General scenario:

$$P_1 \not\approx_{\text{behav}} P_2 \;\text{ iff }\; P_2 \vdash \phi,\; P_2 \not\vdash \phi \qquad \text{for some property } \phi$$

Property ϕ explains why P_1, P_2 behave differently

Counterexample synthesis: automatic

Concurrency workbench MCRL2 UPPAAL ...

Classical case: CCS and HML

$$P_0 = a.(b.\mathbb{0} + c.\mathbb{0})$$
$$Q_0 = a.(b.\mathbb{0} + c.\mathbb{0}) + a.b.\mathbb{0}$$

$$P_0 \not\approx_{\mathsf{bisim}} Q_0$$

Explanation:

$$P_0 \models [a]\langle c\rangle \mathtt{true}$$
$$Q_0 \not\models [a]\langle c\rangle \mathtt{true}$$

$P_0 \models$ whenever a is performed c can subsequently be performed

Classical case: CCS and HML

$$\begin{aligned} P_0 &= a.(b.\mathbb{0} + c.\mathbb{0}) \\ Q_0 &= a.(b.\mathbb{0} + c.\mathbb{0}) + a.b.\mathbb{0} \end{aligned}$$

$$P_0 \not\approx_{\mathsf{bisim}} Q_0$$

Explanation:

$$\begin{aligned} P_0 &\models [a]\,\langle c\rangle\,\mathtt{true} \\ Q_0 &\not\models [a]\,\langle c\rangle\,\mathtt{true} \end{aligned}$$

$P_0 \models$ whenever a is performed c can subsequently be performed

$TCCS^m$: Cooperating transactions

Syntax:

$$
\begin{array}{llll}
P, Q & ::= & \sum \mu_i.P_i & \text{guarded choice} \\
 & \mid & P \mid Q & \text{parallel} \\
 & \mid & \nu a P & \text{hiding} \\
 & \mid & \mathtt{rec} X.P & \text{recursion} \\
 & \mid & [\![P \triangleright_k Q]\!] & \text{running transaction named } k \\
 & \mid & \mathtt{co} & \text{commit}
\end{array}
$$

Transaction $[\![P \triangleright_k Q]\!]$

- execute P to completion (to execution of $\mathtt{co}$)
- subject to random aborts
- if aborted, roll back all effects of P and initiate Q
- roll back includes . . . environmental impact of P

$TCCS^m$: Cooperating transactions

Syntax:

$$
\begin{array}{rcll}
P, Q & ::= & \sum \mu_i.P_i & \text{guarded choice} \\
 & \mid & P \mid Q & \text{parallel} \\
 & \mid & \nu a P & \text{hiding} \\
 & \mid & \mathtt{rec} X.P & \text{recursion} \\
 & \mid & [\![P \triangleright_k Q]\!] & \text{running transaction named } k \\
 & \mid & \mathtt{co} & \text{commit}
\end{array}
$$

Transaction $[\![P \triangleright_k Q]\!]$

- execute P to completion (to execution of $\mathtt{co}$)
- subject to random aborts
- if aborted, roll back all effects of P and initiate Q
- roll back includes . . . environmental impact of P

$TCCS^m$: Cooperating transactions

$$
\begin{array}{llll}
\text{Syntax:} \quad P, Q & ::= & \sum \mu_i.P_i & \text{guarded choice} \\
 & \mid & P \mid Q & \text{parallel} \\
 & \mid & \nu a P & \text{hiding} \\
 & \mid & \mathtt{rec} X.P & \text{recursion} \\
 & \mid & [\![P \triangleright_k Q]\!] & \text{running transaction named } k \\
 & \mid & \mathtt{co} & \text{commit}
\end{array}
$$

Transaction $[\![P \triangleright_k Q]\!]$

- execute P to completion (to execution of $\mathtt{co}$)
- subject to random aborts
- if aborted, roll back all effects of P and initiate Q
- roll back includes . . . environmental impact of P

Rollbacks and Commits

Co-operating actions: $\boxed{a \leftarrow \text{needs co-operation of} \rightarrow \overline{a}}$

$$T_a \mid T_b \mid T_c \mid P_d \mid P_e$$

where

$$\begin{aligned}
T_a &= [\![\overline{d}.\overline{b}.(\mathrm{co} \mid a) \triangleright_{k_1} \mathbb{0}]\!] \\
T_b &= [\![\overline{c}.(\mathrm{co} \mid b) \triangleright_{k_2} \mathbb{0}]\!] \\
T_c &= [\![\overline{e}.c.\mathrm{co} \triangleright_{k_3} \mathbb{0}]\!] \\
P_d &= d.R_d \\
P_e &= e.R_e
\end{aligned}$$

- if T_c aborts, what roll-backs are necessary?
- When can action a be considered permanent?
- When can code P_d be considered permanent?

Rollbacks and Commits

Co-operating actions: $\boxed{a \leftarrow \text{needs co-operation of} \rightarrow \overline{a}}$

$$T_a \mid T_b \mid T_c \mid P_d \mid P_e$$

where

$$\begin{aligned} T_a &= [\![\overline{d}.\overline{b}.(\mathsf{co} \mid a) \rhd_{k_1} \mathbf{0}]\!] \\ T_b &= [\![\overline{c}.(\mathsf{co} \mid b) \rhd_{k_2} \mathbf{0}]\!] \\ T_c &= [\![\overline{e}.c.\mathsf{co} \rhd_{k_3} \mathbf{0}]\!] \\ P_d &= d.R_d \\ P_e &= e.R_e \end{aligned}$$

- if T_c aborts, what roll-backs are necessary?
- When can action a be considered permanent?
- When can code P_d be considered permanent?

Rollbacks and Commits

Co-operating actions: $\boxed{a \leftarrow \text{needs co-operation of} \rightarrow \overline{a}}$

$$T_a \mid T_b \mid T_c \mid P_d \mid P_e$$

where

$$\begin{aligned}
T_a &= \llbracket \overline{d}.\overline{b}.(\mathrm{co} \mid a) \triangleright_{k_1} \mathbf{0} \rrbracket \\
T_b &= \llbracket \overline{c}.(\mathrm{co} \mid b) \triangleright_{k_2} \mathbf{0} \rrbracket \\
T_c &= \llbracket \overline{e}.c.\mathrm{co} \triangleright_{k_3} \mathbf{0} \rrbracket \\
P_d &= d.R_d \\
P_e &= e.R_e
\end{aligned}$$

- if T_c aborts, what roll-backs are necessary?
- When can action a be considered permanent?
- When can code P_d be considered permanent?

Examples

Independent activity:

$$\mathtt{rec}X.\,[\![a.b.\mathrm{co} \rhd_{k_1} X]\!] \mid \mathtt{rec}Y.\,[\![c.d.\mathrm{co} \rhd_{k_2} Y]\!]$$

Dependent activity:

$$(\nu p)\,\mathtt{rec}X.\,[\![a.b.p.\mathrm{co} \rhd_{k_1} X]\!] \mid \mathtt{rec}Y.\,[\![c.d.\overline{p}.\mathrm{co} \rhd_{k_2} Y]\!]$$

Very dependent activity:

$$(\nu p, q)\,\mathtt{rec}X.\,[\![a.q.b.p.\mathrm{co} \rhd_{k_1} X]\!] \mid \mathtt{rec}Y.\,[\![c.\overline{q}.d.\overline{p}.\mathrm{co} \rhd_{k_2} Y]\!]$$

Examples

Independent activity:

$$\mathtt{rec}X.\,[\![a.b.\mathrm{co} \rhd_{k_1} X]\!] \mid \mathtt{rec}Y.\,[\![c.d.\mathrm{co} \rhd_{k_2} Y]\!]$$

Dependent activity:

$$(\nu p)\,\mathtt{rec}X.\,[\![a.b.p.\mathrm{co} \rhd_{k_1} X]\!] \mid \mathtt{rec}Y.\,[\![c.d.\overline{p}.\mathrm{co} \rhd_{k_2} Y]\!]$$

Very dependent activity:

$$(\nu p, q)\,\mathtt{rec}X.\,[\![a.q.b.p.\mathrm{co} \rhd_{k_1} X]\!] \mid \mathtt{rec}Y.\,[\![c.\overline{q}.d.\overline{p}.\mathrm{co} \rhd_{k_2} Y]\!]$$

TRINITY COLLEGE DUBLIN
Coláiste na Tríonóide, Baile Átha Cliath

Examples

Independent activity:

$$\mathtt{rec}X.\,[\![a.b.\mathsf{co} \rhd_{k_1} X]\!] \mid \mathtt{rec}Y.\,[\![c.d.\mathsf{co} \rhd_{k_2} Y]\!]$$

Dependent activity:

$$(\nu p)\,\mathtt{rec}X.\,[\![a.b.p.\mathsf{co} \rhd_{k_1} X]\!] \mid \mathtt{rec}Y.\,[\![c.d.\overline{p}.\mathsf{co} \rhd_{k_2} Y]\!]$$

Very dependent activity:

$$(\nu p, q)\,\mathtt{rec}X.\,[\![a.q.b.p.\mathsf{co} \rhd_{k_1} X]\!] \mid \mathtt{rec}Y.\,[\![c.\overline{q}.d.\overline{p}.\mathsf{co} \rhd_{k_2} Y]\!]$$

Tentative vs Permanent actions

for bisimulations

$$[\![a.b.\textcolor{red}{\mathsf{co}} + a.c.\textcolor{red}{\mathbb{0}} \triangleright_k \mathbb{0}]\!] \xrightarrow{k(a)} \quad \text{tentative } a$$

$$\xrightarrow{k(b)} \quad \text{tentative } b$$

Tentative vs Permanent actions

for bisimulations

$$[\![a.b.\mathsf{co} + a.c.\mathbb{0} \triangleright_k \mathbb{0}]\!] \xrightarrow{a} \quad \text{permanent } a$$

$$\xrightarrow{b} \quad \text{permanent } b$$

$$\xrightarrow{\mathsf{co}\,k} \quad \text{commit } k$$

$$[\![a.b.\mathsf{co} + a.c.\mathbb{0} \triangleright_k \mathbb{0}]\!] \xrightarrow{k(a)} \quad \text{tentative } a$$

$$\xrightarrow{k(c)} \quad \text{tentative } c$$

Tentative vs Permanent actions

for bisimulations

$$[\![a.b.\mathrm{co} + a.c.\mathbb{0} \rhd_k \mathbb{0}]\!] \xrightarrow{a} \quad \text{permanent } a$$

$$\xrightarrow{b} \quad \text{permanent } b$$

$$\xrightarrow{\mathrm{co}\,k} \quad \text{commit } k$$

$$[\![a.b.\mathrm{co} + a.c.\mathbb{0} \rhd_k \mathbb{0}]\!] \xrightarrow{k(a)} \quad \text{tentative } a$$

$$\xrightarrow{k(c)} \quad \text{tentative } c$$

TRINITY COLLEGE DUBLIN

Remembering via Histories: $H \triangleright P$

$$\varepsilon \;\triangleright\; [\![a.p.\mathrm{co} \triangleright_k \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} \triangleright_l \mathbf{0}]\!] \xrightarrow{k_1(a)}$$

tentative a $\quad$ k_1 fresh

$$\mathrm{Id}; k_1(a) \;\triangleright\; [\![p.\mathrm{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} \triangleright_l \mathbf{0}]\!] \xrightarrow{k_2(b)}$$

tentative b $\quad$ k_2 fresh

$$\mathrm{Id}; k_1(a).\,k_2(b) \;\triangleright\; [\![p.\mathrm{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![\overline{p}.\mathrm{co} \triangleright_{k_2} \mathbf{0}]\!] \xrightarrow{\tau}$$

comm = merging $\quad$ k_3 fresh

$$\{k_1, k_2, k_3\}; k_1(a).\,k_2(b) \;\triangleright\; [\![\mathrm{co} \triangleright_{k_3} \mathbf{0}]\!] \mid [\![\mathrm{co} \triangleright_{k_3} \mathbf{0}]\!] \xrightarrow{\tau}$$

committing

$$\{k_1, k_2, k_3\}; k_1(\mathrm{co}).\,k_2(\mathrm{co}) \;\triangleright\; \mathbf{0} \mid \mathbf{0}$$

permanent a, b

TRINITY COLLEGE DUBLIN
COLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH

Remembering via Histories: $H \rhd P$

$$\varepsilon \quad \rhd \quad [\![a.p.\mathsf{co} \rhd_k \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathsf{co} \rhd_l \mathbf{0}]\!] \quad \xrightarrow{k_1(a)}$$

tentative a $\quad$ k_1 fresh

$$\mathrm{Id}; k_1(a) \quad \rhd \quad [\![p.\mathsf{co} \rhd_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathsf{co} \rhd_l \mathbf{0}]\!] \quad \xrightarrow{k_2(b)}$$

tentative b $\quad$ k_2 fresh

$$\mathrm{Id}; k_1(a).\, k_2(b) \quad \rhd \quad [\![p.\mathsf{co} \rhd_{k_1} \mathbf{0}]\!] \mid [\![\overline{p}.\mathsf{co} \rhd_{k_2} \mathbf{0}]\!] \quad \xrightarrow{\tau}$$

comm = merging $\quad$ k_3 fresh

$$\{k_1, k_2, k_3\}; k_1(a).\, k_2(b) \quad \rhd \quad [\![\mathsf{co} \rhd_{k_3} \mathbf{0}]\!] \mid [\![\mathsf{co} \rhd_{k_3} \mathbf{0}]\!] \quad \xrightarrow{\tau}$$

committing

$$\{k_1, k_2, k_3\}; k_1(\mathsf{co}).\, k_2(\mathsf{co}) \quad \rhd \quad \mathbf{0} \mid \mathbf{0}$$

permanent a, b

Remembering via Histories: $H \rhd P$

$$\varepsilon \quad \rhd \quad [\![a.p.\mathrm{co} \rhd_k \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} \rhd_l \mathbf{0}]\!] \quad \xrightarrow{k_1(a)}$$

tentative a k_1 fresh

$$\mathrm{Id};\, k_1(a) \quad \rhd \quad [\![p.\mathrm{co} \rhd_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} \rhd_l \mathbf{0}]\!] \quad \xrightarrow{k_2(b)}$$

tentative b k_2 fresh

$$\mathrm{Id};\, k_1(a).\, k_2(b) \quad \rhd \quad [\![p.\mathrm{co} \rhd_{k_1} \mathbf{0}]\!] \mid [\![\overline{p}.\mathrm{co} \rhd_{k_2} \mathbf{0}]\!] \quad \xrightarrow{\tau}$$

comm = merging k_3 fresh

$$\{k_1, k_2, k_3\};\, k_1(a).\, k_2(b) \quad \rhd \quad [\![\mathrm{co} \rhd_{k_3} \mathbf{0}]\!] \mid [\![\mathrm{co} \rhd_{k_3} \mathbf{0}]\!] \quad \xrightarrow{\tau}$$

committing

$$\{k_1, k_2, k_3\};\, k_1(\mathrm{co}).\, k_2(\mathrm{co}) \quad \rhd \quad \mathbf{0} \mid \mathbf{0}$$

permanent a, b

Remembering via Histories: $H \triangleright P$

$$\varepsilon \quad \triangleright \quad [\![a.p.\mathrm{co} \triangleright_k \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} \triangleright_l \mathbf{0}]\!] \quad \xrightarrow{k_1(a)}$$

tentative a k_1 fresh

$$\mathrm{Id}; k_1(a) \quad \triangleright \quad [\![p.\mathrm{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} \triangleright_l \mathbf{0}]\!] \quad \xrightarrow{k_2(b)}$$

tentative b k_2 fresh

$$\mathrm{Id}; k_1(a).\, k_2(b) \quad \triangleright \quad [\![p.\mathrm{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![\overline{p}.\mathrm{co} \triangleright_{k_2} \mathbf{0}]\!] \quad \xrightarrow{\tau}$$

comm = merging k_3 fresh

$$\{k_1, k_2, k_3\}; k_1(a).\, k_2(b) \quad \triangleright \quad [\![\mathrm{co} \triangleright_{k_3} \mathbf{0}]\!] \mid [\![\mathrm{co} \triangleright_{k_3} \mathbf{0}]\!] \quad \xrightarrow{\tau}$$

committing

$$\{k_1, k_2, k_3\}; k_1(\mathrm{co}).\, k_2(\mathrm{co}) \quad \triangleright \quad \mathbf{0} \mid \mathbf{0}$$

permanent a, b

Remembering via Histories: $H \triangleright P$

$$\varepsilon \quad \triangleright \quad [\![a.p.\mathrm{co} \triangleright_k \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} \triangleright_l \mathbf{0}]\!] \xrightarrow{k_1(a)}$$

tentative a $\quad$ k_1 fresh

$$\mathrm{Id}; k_1(a) \quad \triangleright \quad [\![p.\mathrm{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} \triangleright_l \mathbf{0}]\!] \xrightarrow{k_2(b)}$$

tentative b $\quad$ k_2 fresh

$$\mathrm{Id}; k_1(a).\, k_2(b) \quad \triangleright \quad [\![p.\mathrm{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![\overline{p}.\mathrm{co} \triangleright_{k_2} \mathbf{0}]\!] \xrightarrow{\tau}$$

comm = merging $\quad$ k_3 fresh

$$\{k_1, k_2, k_3\}; k_1(a).\, k_2(b) \quad \triangleright \quad [\![\mathrm{co} \triangleright_{k_3} \mathbf{0}]\!] \mid [\![\mathrm{co} \triangleright_{k_3} \mathbf{0}]\!] \xrightarrow{\tau}$$

committing

$$\{k_1, k_2, k_3\}; k_1(\mathrm{co}).\, k_2(\mathrm{co}) \quad \triangleright \quad \mathbf{0} \mid \mathbf{0}$$

permanent a, b

Remembering via Histories: $H \triangleright P$

$$\varepsilon \quad \triangleright \quad [\![a.p.\mathrm{co} \triangleright_k \mathbb{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} \triangleright_l \mathbb{0}]\!] \quad \xrightarrow{k_1(a)}$$

tentative a k_1 fresh

$$\mathrm{Id}; k_1(a) \quad \triangleright \quad [\![p.\mathrm{co} \triangleright_{k_1} \mathbb{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} \triangleright_l \mathbb{0}]\!] \quad \xrightarrow{k_2(b)}$$

tentative b k_2 fresh

$$\mathrm{Id}; k_1(a).\, k_2(b) \quad \triangleright \quad [\![p.\mathrm{co} \triangleright_{k_1} \mathbb{0}]\!] \mid [\![\overline{p}.\mathrm{co} \triangleright_{k_2} \mathbb{0}]\!] \quad \xrightarrow{\tau}$$

comm = merging k_3 fresh

$$\{k_1, k_2, k_3\}; k_1(a).\, k_2(b) \quad \triangleright \quad [\![\mathrm{co} \triangleright_{k_3} \mathbb{0}]\!] \mid [\![\mathrm{co} \triangleright_{k_3} \mathbb{0}]\!] \quad \xrightarrow{\tau}$$

committing

$$\{k_1, k_2, k_3\}; k_1(\mathrm{co}).\, k_2(\mathrm{co}) \quad \triangleright \quad \mathbb{0} \mid \mathbb{0}$$

permanent a, b

Configurations: $H \triangleright P$

where H remembers

- tentative actions what commits they depend on
- aborted transactions
- committed transactions
- equivalence between transaction names

Configurations: $H \triangleright P$

where H remembers

- tentative actions what commits they depend on
- aborted transactions
- committed transactions
- equivalence between transaction names

Bisimulations

$$H_1 \triangleright P_1 \approx_{\text{bisim}} H_2 \triangleright P_2$$

whenever

- H_1, H_2 are consistent :
  - committed actions agree

- $H_1 \triangleright P_1 \xrightarrow{\lambda} H_1' \triangleright P_1'$ where λ uses fresh names, implies $H_2 \triangleright P_2 \stackrel{\lambda}{\Rightarrow} H_2' \triangleright P_2'$ such that $H_1' \triangleright P_1 \approx_{\text{bisim}} H_2' \triangleright P_2'$

- ...

Intricacies:

- Commits/aborts treated as internal actions
- Dummy actions allowed

Bisimulations

$$H_1 \triangleright P_1 \approx_{\mathrm{bisim}} H_2 \triangleright P_2$$

whenever

- H_1, H_2 are consistent :
  - committed actions agree
- $H_1 \triangleright P_1 \xrightarrow{\lambda} H_1' \triangleright P_1'$ where λ uses fresh names, implies $H_2 \triangleright P_2 \stackrel{\lambda}{\Rightarrow} H_2' \triangleright P_2'$ such that $H_1' \triangleright P_1 \approx_{\mathrm{bisim}} H_2' \triangleright P_2'$
- ...

Intricacies:

- Commits/aborts treated as internal actions
- Dummy actions allowed

Using logic

$$P_1 = [\![a.(b.co + c.co) \triangleright_k \mathbf{0}]\!]$$
$$Q_1 = [\![a.b.co + a.c.\mathbf{0}) \triangleright_l \mathbf{0}]\!]$$

Distinguishing property:

$$P_1 \models \langle x(a)\rangle \langle y(c)\rangle \mathtt{Hasco}(y)$$
$$Q_1 \not\models \ldots\ldots$$

Explanation:

P_1 can

- execute a in some transaction
- then execute c is some other transaction
- reach a state in which second transaction is committed

Using logic

$$P_1 = [\![a.(b.\mathrm{co} + c.\mathrm{co}) \triangleright_k \mathbb{0}]\!]$$
$$Q_1 = [\![a.b.\mathrm{co} + a.c.\mathbb{0}) \triangleright_l \mathbb{0}]\!]$$

Distinguishing property:

$$P_1 \models \langle x(a)\rangle \langle y(c)\rangle \mathtt{Hasco}(y)$$
$$Q_1 \not\models \ldots\ldots$$

Explanation:

P_1 can

- execute a in some transaction
- then execute c is some other transaction
- reach a state in which second transaction is committed

TRINITY COLLEGE DUBLIN

Using logic

$$
\begin{aligned}
P_1 &= [\![a.(b.\mathrm{co} + c.\mathrm{co}) \triangleright_k \mathbb{0}]\!] \\
Q_1 &= [\![a.b.\mathrm{co} + a.c.\mathbb{0}) \triangleright_l \mathbb{0}]\!]
\end{aligned}
$$

Distinguishing property:

$$
\begin{aligned}
P_1 &\models \langle x(a) \rangle \langle y(c) \rangle \, \mathtt{Hasco}(y) \\
Q_1 &\not\models \ldots\ldots
\end{aligned}
$$

Explanation:

P_1 can

- execute a in some transaction
- then execute c is some other transaction
- reach a state in which second transaction is committed

TRINITY COLLEGE DUBLIN

Property logics

$$
\begin{aligned}
\phi \in \mathcal{L} \quad ::= &\quad \langle x(a) \rangle\, \phi, \quad x \in \mathrm{Var} \\
&\quad \mid\ \bigwedge_{\{i \in I\}} \phi_i \mid \neg\phi \mid \langle \tau \rangle\, \phi \\
&\quad \mid \text{some predicates on} \ldots \\
v \in \mathrm{Values} \quad ::= &\quad k \in \mathrm{TrName}\ \ _{\text{constants}} \mid x \in \mathrm{Var}\ \ _{\text{variables}}
\end{aligned}
$$

Nominal Interpretation: à la Pitts Gabbay

$H \rhd P \models \langle x(a) \rangle\, \phi$ if

- for almost all $k \in \mathrm{TrName}$
- $H \rhd P \xRightarrow{k(a)} H' \rhd P' \models \phi$

One useful predicate:

$H \rhd P \models \mathtt{Hasco}(k)$ if

- $l(\mathrm{co})$ is in H
- for some l equivalent to k

Property logics

$$\begin{aligned} \phi \in \mathcal{L} \quad ::= \quad & \langle x(a) \rangle \, \phi, \quad x \in \mathrm{Var} \\ & \mid \; \textstyle\bigwedge_{\{i \in I\}} \phi_i \mid \neg\phi \mid \; \langle \tau \rangle \, \phi \\ & \mid \text{some predicates on} \ldots \\ v \in \mathrm{Values} \quad ::= \quad & k \in \mathrm{TrName} \;\; {}_{\text{constants}} \mid x \in \mathrm{Var} \;\; {}_{\text{variables}} \end{aligned}$$

Nominal Interpretation: à la Pitts Gabbay

$H \triangleright P \models \langle x(a) \rangle \, \phi$ if

- for almost all $k \in \mathrm{TrName}$
- $H \triangleright P \xRightarrow{k(a)} H' \triangleright P' \models \phi$

One useful predicate:

$H \triangleright P \models \mathtt{Hasco}(k)$ if

- $l(\mathrm{co})$ is in H
- for some l equivalent to k

TRINITY COLLEGE DUBLIN

Property logics

$$
\begin{aligned}
\phi \in \mathcal{L} \quad &::= \quad \langle x(a) \rangle\, \phi, \quad x \in \mathrm{Var} \\
&\qquad \mid\ \textstyle\bigwedge_{\{i \in I\}} \phi_i \mid \neg\phi \mid\ \langle \tau \rangle\, \phi \\
&\qquad \mid \text{some predicates on} \ldots \\
v \in \mathrm{Values} \quad &::= \quad k \in \mathrm{TrName} \ \ {}_{\text{constants}} \mid x \in \mathrm{Var} \ \ {}_{\text{variables}}
\end{aligned}
$$

Nominal Interpretation: à la Pitts Gabbay

$H \rhd P \models \langle x(a) \rangle\, \phi$ if

- for almost all $k \in \mathrm{TrName}$
- $H \rhd P \xRightarrow{k(a)} H' \rhd P' \models \phi$

One useful predicate:

$H \rhd P \models \mathtt{Hasco}(k)$ if

- $l(\mathrm{co})$ is in H
- for some l equivalent to k

An example

$$
\begin{aligned}
P_2 &= \llbracket a.b.\mathrm{co} + b.a.\mathrm{co}) \triangleright_k \mathbb{0} \rrbracket \\
Q_2 &= \llbracket a.\mathrm{co} \triangleright_{k_1} \mathbb{0} \rrbracket \mid \llbracket b.\mathrm{co} \triangleright_{k_2} \mathbb{0} \rrbracket
\end{aligned}
$$

Distinguishing property:

$$
\begin{aligned}
P_2 &\models \langle x(a) \rangle \langle y(b) \rangle\, x = y \\
Q_2 &\not\models \ldots\ldots
\end{aligned}
$$

Intuition: P_2 can execute both actions in same transaction

Semantics:
$H \triangleright P \models k_1 = k_2$ if

- k_1, k_2 are equivalent in H
- both k_1, k_2 are committed in H

TRINITY COLLEGE DUBLIN
COLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH

An example

$$P_2 = [\![a.b.co + b.a.co) \triangleright_k \mathbf{0}]\!]$$
$$Q_2 = [\![a.co \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.co \triangleright_{k_2} \mathbf{0}]\!]$$

Distinguishing property:

$$P_2 \models \langle x(a) \rangle \langle y(b) \rangle\, x = y$$
$$Q_2 \not\models \ldots\ldots$$

Intuition: P_2 can execute both actions in same transaction

Semantics:

$H \triangleright P \models k_1 = k_2$ if

- k_1, k_2 are equivalent in H
- both k_1, k_2 are committed in H

An example

$$
\begin{aligned}
P_2 &= [\![a.b.\mathrm{co} + b.a.\mathrm{co}) \triangleright_k \mathbf{0}]\!] \\
Q_2 &= [\![a.\mathrm{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\mathrm{co} \triangleright_{k_2} \mathbf{0}]\!]
\end{aligned}
$$

Distinguishing property:

$$
\begin{aligned}
P_2 &\models \langle x(a)\rangle \langle y(b)\rangle\, x = y \\
Q_2 &\not\models \;\ldots\ldots
\end{aligned}
$$

Intuition: P_2 can execute both actions in same transaction

Semantics:

$H \triangleright P \models k_1 = k_2$ if

- k_1, k_2 are equivalent in H
- both k_1, k_2 are committed in H

An example

$$P_3 = \nu p.\ [\![a.p.\mathrm{co} + a.\mathrm{co}) \rhd_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} + b.\mathrm{co}) \rhd_{k_2} \mathbf{0}]\!]$$
$$Q_3 = [\![a.\mathrm{co} \rhd_{k_1} \mathbf{0}]\!] \mid [\![b.\mathrm{co} \rhd_{k_2} \mathbf{0}]\!]$$

Distinguishing property:

P_3 can

- perform a followed by b in two distinct transactions
- then can simultaneously commit both

Logic:

- $P_3 \models_{\mathrm{CC}} \langle x(a)\rangle \langle y(b)\rangle \langle \mathrm{co}(\{x,y\})\rangle\, \mathtt{true}$.
- $Q_3 \not\models_{\mathrm{CC}} \ldots\ldots$

An example

$$
\begin{aligned}
P_3 &= \nu p.\ [\![a.p.\mathrm{co} + a.\mathrm{co}) \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} + b.\mathrm{co}) \triangleright_{k_2} \mathbf{0}]\!] \\
Q_3 &= [\![a.\mathrm{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\mathrm{co} \triangleright_{k_2} \mathbf{0}]\!]
\end{aligned}
$$

Distinguishing property:

P_3 can

- perform a followed by b in two distinct transactions
- then can simultaneously commit both

Logic:

- $P_3 \models_{cc} \langle x(a) \rangle \langle y(b) \rangle \langle \mathrm{co}(\{x, y\}) \rangle\, \mathtt{true}$.
- $Q_3 \not\models_{cc} \ldots\ldots$

An example

$$
\begin{aligned}
P_3 &= \nu p.\ [\![a.p.\mathrm{co} + a.\mathrm{co}) \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} + b.\mathrm{co}) \triangleright_{k_2} \mathbf{0}]\!] \\
Q_3 &= [\![a.\mathrm{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\mathrm{co} \triangleright_{k_2} \mathbf{0}]\!]
\end{aligned}
$$

Distinguishing property:

P_3 can

- perform a followed by b in two distinct transactions
- then can simultaneously commit both

Logic:

- $P_3 \models_{\mathrm{CC}} \langle x(a)\rangle\, \langle y(b)\rangle\, \langle \mathrm{co}(\{x, y\})\rangle\, \texttt{true}.$
- $Q_3 \not\models_{\mathrm{CC}} \ldots\ldots$

Simultaneous commits

$$P_3 = \nu p.\ [\![a.p.\mathsf{co} + a.\mathsf{co}) \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathsf{co} + b.\mathsf{co}) \triangleright_{k_2} \mathbf{0}]\!]$$
$$Q_3 = [\![a.\mathsf{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\mathsf{co} \triangleright_{k_2} \mathbf{0}]\!]$$

Distinguishing property:

P_3 can

- perform a followed by b in two distinct transactions
- then can simultaneously commit both
- $\langle x(a)\rangle \langle y(b)\rangle \langle \mathsf{co}(\{x,y\})\rangle\, \mathtt{true}$

Semantics:

$H \triangleright P \models \langle \mathsf{co}(K)\rangle\, \phi$ if

- $H \triangleright P \overset{\tau}{\Rightarrow} H' \triangleright P' \xrightarrow{\mathsf{co}(m)} \overset{\tau}{\Rightarrow} H'' \triangleright P'' \models \phi$
- every k in K is equivalent to m in H'

Simultaneous commits

$$P_3 = \nu p.\ [\![a.p.\mathrm{co} + a.\mathrm{co}) \rhd_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} + b.\mathrm{co}) \rhd_{k_2} \mathbf{0}]\!]$$
$$Q_3 = [\![a.\mathrm{co} \rhd_{k_1} \mathbf{0}]\!] \mid [\![b.\mathrm{co} \rhd_{k_2} \mathbf{0}]\!]$$

Distinguishing property:

P_3 can

- perform a followed by b in two distinct transactions
- then can simultaneously commit both
- $\langle x(a)\rangle \langle y(b)\rangle \langle \mathrm{co}(\{x,y\})\rangle\, \mathtt{true}$

Semantics:

$H \rhd P \models \langle \mathrm{co}(K)\rangle\, \phi$ if

- $H \rhd P \stackrel{\tau}{\Rightarrow} H' \rhd P' \xrightarrow{\mathrm{co}(m)} \stackrel{\tau}{\Rightarrow} H'' \rhd P'' \models \phi$
- every k in K is equivalent to m in H'

Simultaneous commits

$$P_3 = \nu p.\ [\![a.p.\mathrm{co} + a.\mathrm{co}) \triangleright_{k_1} \mathbb{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} + b.\mathrm{co}) \triangleright_{k_2} \mathbb{0}]\!]$$
$$Q_3 = [\![a.\mathrm{co} \triangleright_{k_1} \mathbb{0}]\!] \mid [\![b.\mathrm{co} \triangleright_{k_2} \mathbb{0}]\!]$$

Distinguishing property:

P_3 can

- perform a followed by b in two distinct transactions
- then can simultaneously commit both
- $\langle x(a)\rangle\,\langle y(b)\rangle\,\langle \mathrm{co}(\{x,y\})\rangle\,\mathtt{true}$

Semantics:

$H \triangleright P \models \langle \mathrm{co}(K)\rangle\,\phi$ if

- $H \triangleright P \stackrel{\tau}{\Rightarrow} H' \triangleright P' \xrightarrow{\mathrm{co}(m)} \stackrel{\tau}{\Rightarrow} H'' \triangleright P'' \models \phi$
- every k in K is equivalent to m in H'

Simultaneous commits

$$P_3 = \nu p.\ [\![a.p.\mathrm{co} + a.\mathrm{co}) \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\overline{p}.\mathrm{co} + b.\mathrm{co}) \triangleright_{k_2} \mathbf{0}]\!]$$

$$Q_3 = [\![a.\mathrm{co} \triangleright_{k_1} \mathbf{0}]\!] \mid [\![b.\mathrm{co} \triangleright_{k_2} \mathbf{0}]\!]$$

Distinguishing property:

P_3 can

- perform a followed by b in two distinct transactions
- then can simultaneously commit both
- $\langle x(a)\rangle \, \langle y(b)\rangle \, \langle \mathrm{co}(\{x, y\})\rangle \, \mathtt{true}$

Semantics:

$H \triangleright P \models \langle \mathrm{co}(K)\rangle \, \phi$ if

- $H \triangleright P \stackrel{\tau}{\Rightarrow} H' \triangleright P' \xrightarrow{\mathrm{co}(m)} \stackrel{\tau}{\Rightarrow} H'' \triangleright P'' \models \phi$
- every k in K is equivalent to m in H'

Three logics

- $\mathcal{L}_{\text{Hasco}}$: nominal HML + property $\mathtt{Hasco}$ has committed
- $\mathcal{L}_{\text{Eq}}$: nominal HML + equality property $v_1 = v_2$
- $\mathcal{L}_{\text{Canco}}$:
  - No properties
  - nominal HML + $\langle \mathrm{co}(K) \rangle\, \phi$ simultaneous commits

Main results:

- all three logics capture contextual equivalence
- All three logics are equally expressive

TRINITY COLLEGE DUBLIN

Three logics

- $\mathcal{L}_{\text{Hasco}}$: nominal HML + property $\texttt{Hasco}$ has committed
- $\mathcal{L}_{\text{Eq}}$: nominal HML + equality property $v_1 = v_2$
- $\mathcal{L}_{\text{Canco}}$:
  - No properties
  - nominal HML + $\langle \mathrm{co}(K) \rangle \, \phi$ simultaneous commits

Main results:

- all three logics capture contextual equivalence
- All three logics are equally expressive

Expressiveness

Weak:

$$\begin{aligned} P \approx_{\mathsf{cxt}} Q \quad & \text{iff} \quad \mathcal{L}_{\mathsf{Hasco}}(P) = \mathcal{L}_{\mathsf{Hasco}}(Q) \\ & \text{iff} \quad \mathcal{L}_{\mathsf{Eq}}(P) = \mathcal{L}_{\mathsf{Eq}}(Q) \\ & \text{iff} \quad \mathcal{L}_{\mathsf{Canco}}(P) = \mathcal{L}_{\mathsf{Canco}}(Q) \end{aligned}$$

Strong:

For all $\phi \in \mathcal{L}_X$ there is some $\mathsf{tr}(\phi) \in \mathcal{L}_Y$ such that

$$P \models \phi \quad \Longleftrightarrow \quad P \models \mathsf{tr}(\phi)$$

THE END

THANK YOU