†

‡

These notes are intended to support the course on Semantics and Verification, and may be read independently or in conjunction with Milner's textbook [15]. They are under constant revision, and their most recent version is available at the URL

http://www.cs.auc.dk/ luca/SV/intro2ccs.pdf.

Please let us know of any comment you may have, or typographical mistake you may find, by sending an email at the addresses

`luca@cs.aau.dk` and `srba@cs.aau.dk`

with subject line "CCS Notes".

Contents

1 Introduction **2**

2 What Are Reactive Systems? **4**

3 Process Algebras **7**

*

†

‡

4 The Language CCS 8

5 Behavioural Equivalence 30

6 Hennessy-Milner Logic 63

7 Hennessy-Milner Logic with Recursive De initions 73

A Theory of Fixed Points and Tarski's Fixed Point Theorem 104

1 Introduction

Semantics and Verification

-
-
-

Semantics and Verification

2 What Are Reactive Systems?

algo-rithmic problem

state

partial

$$S = z \leftarrow x; x \leftarrow y; y \leftarrow z$$

$[\![S]\!]$

$$[\![S]\!] = \lambda s.\ s[x \rightarrow s(y), y \rightarrow s(x), z \rightarrow s(x)]\ ,$$

$s[x \rightarrow s(y), y \rightarrow s(x), z \rightarrow s(x)]$

x y s y z x

s s

S

x y

$$U = \textbf{while}\quad \textbf{do skip}$$

partial

$$[\![U]\!] = \lambda s. \qquad ,$$

U

-
-
-
-

loop

forever

reactive system

desirable

not

!

non-determinism

any

Process Theory

-
-
-
-

3 Process Algebras

process algebra

P Q

P Q

P Q

operation

sender *receiver*

medium

synchronized communication

4 The Language CCS

4.1 Some CCS Process Constructions

process interface

communication ports *channels*

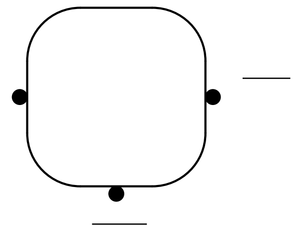
a $\bar{a}$

a *actions*

behaviour

$\mathbf{0}$

$\mathbf{0}$



action prefixing

$\mathbf{0}$

$.\mathbf{0}$

$. \quad .\mathbf{0}$

$\mathbf{0}$ *action*

P a $a.P$

$a.P$

a P

$$= \quad . \quad .\mathbf{0} \; .$$

$$= \quad . \quad .$$

$=$.

$=$ . .

$=$ . . .

$=$,

n

$=$ . . .

choice operator $+$

$=$.(. $+$.) .

P Q $P+Q$

$P+Q$ P Q

P

Q

Exercise 4.1

(1), .

Exercise 4.2 T $(\mathsf{Q}, A, \delta, q_0)$,

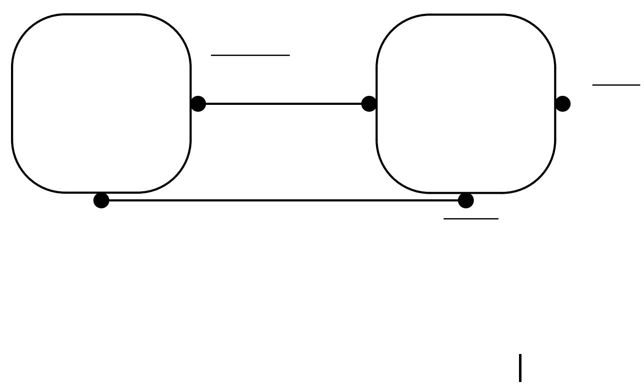
- Q ,
- A ,
- q_0 Q
- $\delta : Q \times A \to 2^Q$.

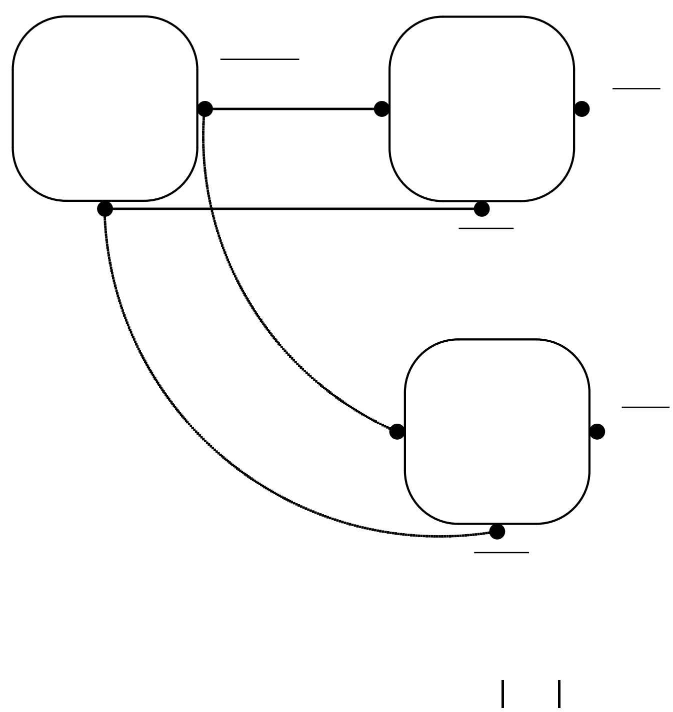
, T .

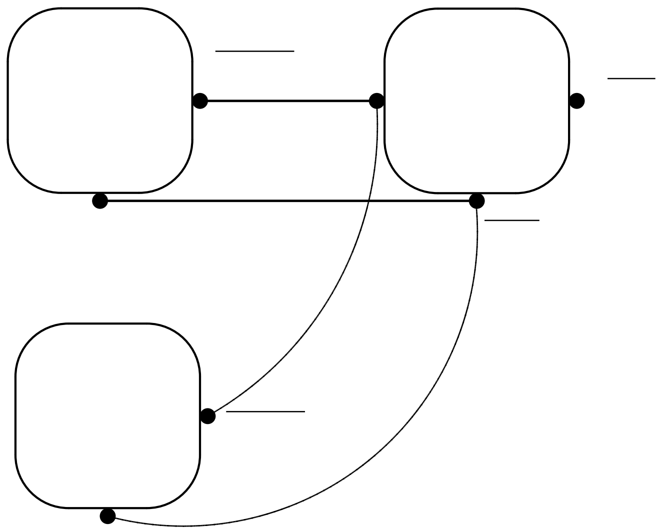
$$= \overline{}.\overline{}. \quad . \quad .$$

parallel composition operation |
|

possible
| *not*







$| \quad |$

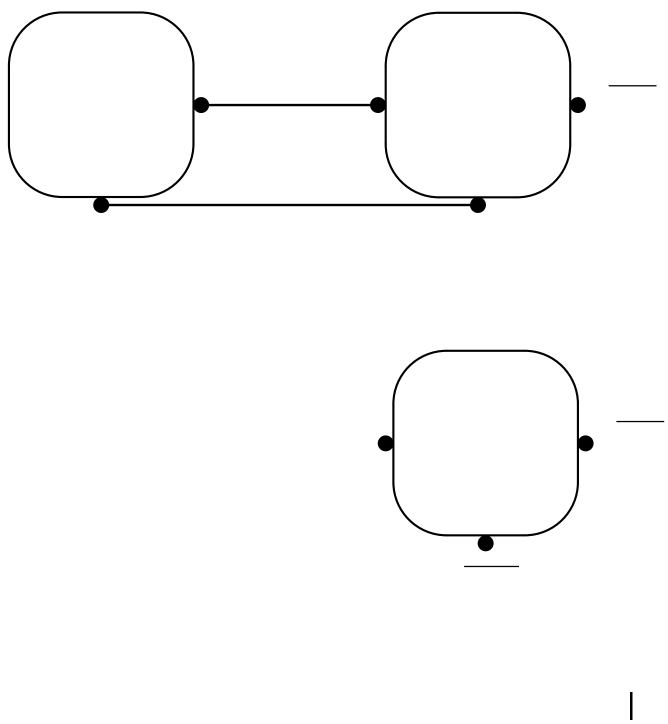
$P \quad Q \quad P\,|\,Q$

- $P \quad Q$
-

restriction

$\backslash \quad \backslash$

$$= (\quad | \quad) \backslash \quad \backslash \quad .$$



P L $P \setminus L$

$P \setminus L$ L P
P

$$= \quad . \overline{\quad\quad} .$$
$$= \quad . \overline{\quad} .$$
$$= \quad . \overline{\quad\quad\quad} . \quad .$$

generic

$$= \quad . \overline{\quad\quad} . \quad .$$

$$= \quad [\quad / \quad] \ ,$$

$[\quad / \quad]$

P f
$P[f]$

4.1.1 The Behaviour of Processes

$$_1 = \overline{} . \qquad .$$

1

$$_2 = \qquad . \quad .$$

$1 \qquad 2$

!

$$\overline{} \to \quad 1 \ ,$$

1

$$\to \quad 1 \to \quad 2 \to \qquad .$$

$$= \quad . \ 1$$

$$_1 = \overline{} . \quad .$$

1

$$1 \xrightarrow{\overline{}} 2 \; ,$$

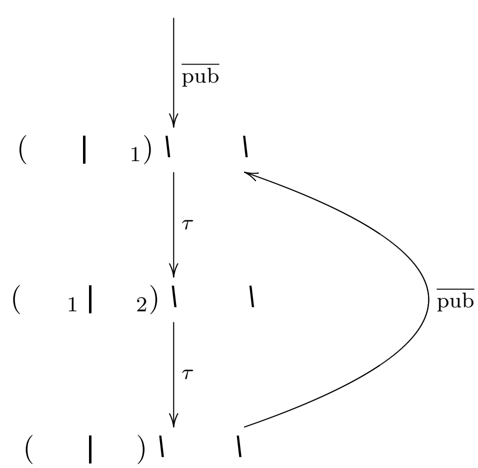
$$\rightarrow \quad 1 \; .$$

$$\mid \quad 1 \xrightarrow{?} \quad 1 \mid \quad 2 \; .$$

hand-shake

new τ

$$\mid \quad 1 \xrightarrow{\tau} \quad 1 \mid \quad 2 \; .$$



τ

$$= \overline{\quad} . \quad .$$

4.2 CCS, Formally

4.2.1 The Model of Labelled Transition Systems

states *processes*
configurations *labels* *actions* $\rightarrow$
p a
p $p \overset{a}{\rightarrow} p$ *start state*

Example 4.1

p

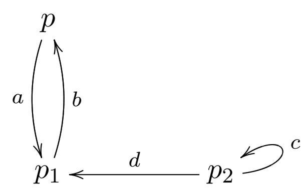
p_1 p_2

$p \to p_1$ $p \to p_2$

p_1 p_2

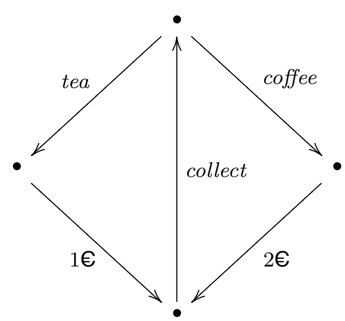
$p_1 \overset{1€}{\to} p_3$ $p_2 \overset{2€}{\to} p_3$

p



p

p



Remark 4.1
p p_2
c
p p_2 p
p
p *reachable* p p p
set of reachable states
p p_1

De inition 4.1 *labelled transition system (LTS)*
$(\mathsf{Proc}, \mathsf{Act}, \{\xrightarrow{a} \mid a \quad \mathsf{Act}\})$

- Proc *states* s
- Act *actions* a
- $\xrightarrow{a}$ Proc × Proc *transition relation* a Act
$s \xrightarrow{a} s$ (s, s) $\xrightarrow{a}$
$s \overset{a}{\nrightarrow}$ s a $s \xrightarrow{a} s$ s

$$
\begin{aligned}
\textsf{Proc} &= \{ \quad ,(\quad | \quad _1) \backslash \quad \backslash \quad ,(\quad _1 | \quad _2) \backslash \quad \backslash \quad , \\
&\quad (\quad | \quad) \backslash \quad \backslash \quad \} \\
\textsf{Act} &= \{ \overline{\quad\quad} , \tau \} \\
\overline{\rightarrow} &= \{(\quad ,(\quad | \quad _1) \backslash \quad \backslash \quad), \\
&\quad ((\quad | \quad) \backslash \quad \backslash \quad ,(\quad | \quad _1) \backslash \quad \backslash \quad)\} \\
\stackrel{\tau}{\rightarrow} &= \{((\quad | \quad _1) \backslash \quad \backslash \quad ,(\quad _1 | \quad _2) \backslash \quad \backslash \quad), \\
&\quad ((\quad _1 | \quad _2) \backslash \quad \backslash \quad ,(\quad | \quad) \backslash \quad \backslash \quad)\} \ .
\end{aligned}
$$

start state *initial state*

Remark 4.2 $\stackrel{a}{\rightarrow}$

$\rightarrow$ $\textsf{Proc} \times \textsf{Act} \times \textsf{Proc}$ $s \stackrel{a}{\rightarrow} s$ $(s, a, s\ )$ $\rightarrow$

Notation 4.1

- $\textsf{Act}$ $\textsf{Act}$ ϵ
  - $s \stackrel{\epsilon}{\rightarrow} s$ s $\textsf{Proc}$
  - $s \stackrel{aw}{\rightarrow} s$ t $\textsf{Proc}$ $s \stackrel{a}{\rightarrow} t$ $t \stackrel{w}{\rightarrow} s$ s, s $\textsf{Proc}$ a $\textsf{Act}$ w $\textsf{Act}$

  $w = a_1 a_2 \cdots a_n$ $a_1, a_2 \ldots, a_n$ $\textsf{Act}$ $s \stackrel{w}{\rightarrow} s$ $s_1, \ldots, s_{n-1}$ $\textsf{Proc}$

  $$s \stackrel{a_1}{\rightarrow} s_1 \stackrel{a_2}{\rightarrow} s_2 \stackrel{a_3}{\rightarrow} s_3 \stackrel{a_4}{\rightarrow} \cdots \stackrel{a_{n-1}}{\rightarrow} s_{n-1} \stackrel{a_n}{\rightarrow} s \quad .$$

  $p \stackrel{\epsilon}{\rightarrow} p$ $p \stackrel{ab}{\rightarrow} p$ $p_1 \stackrel{bab}{\rightarrow} p$
- $s \rightarrow s$ a $\textsf{Act}$ $s \stackrel{a}{\rightarrow} s$

  $p \rightarrow p_1$ $p_1 \rightarrow p$ $p_2 \rightarrow p_1$ $p_2 \rightarrow p_2$

1

- $s \xrightarrow{a}$ s Proc
$s \xrightarrow{a} s$
$p \xrightarrow{a}$
$p_1 \xrightarrow{b}$
- $s \rightarrow s$ $s \xrightarrow{w} s$ w Act $\rightarrow$
$\rightarrow$
$p \rightarrow p$
$p \rightarrow p_1$ $p_2 \rightarrow p$

De inition 4.2 $T = (\mathsf{Proc}, \mathsf{Act}, \{\xrightarrow{a} \mid a \; \mathsf{Act}\})$
s Proc s Proc
reachable in T $s \rightarrow s$ *reachable states*
T

p
$\{p, p_1\}$

Exercise 4.3 -
1 p_2

Structural Operational Se-
mantics

τ

4.2.2 The Formal Syntax and Semantics of CCS

A *(channel)*

names

$$\bar{A} = \{\bar{a} \mid a \quad A\}$$

complementary names

$$L = A \quad \bar{A}$$

labels

$$\mathsf{Act} = L \quad \{\tau\}$$

actions a, b

L

$\bar{\bar{a}} = a$ a

K *process names* *constants*

Definition 4.3 P *CCS expressions*

$$P, Q ::= K \ \mid \ \alpha.P \ \mid \ \sum_{i \ I} P_i \ \mid \ P \mid Q \ \mid \ P[f] \ \mid \ P \setminus L \ ,$$

- K K
- α Act
- I
- $f : \mathsf{Act} \to \mathsf{Act}$ *relabelling function*

$$\begin{aligned} f(\tau) &= \tau \\ f(\bar{a}) &= \overline{f(a)} \end{aligned} \qquad a \ ;$$

- L

$\mathbf{0}$

$$\mathbf{0} = \sum_{i} P_i \ ,$$

$P_1 + P_2$

$$P_1 + P_2 = \sum_{i \in \{1,2\}} P_i \ .$$

$$K \stackrel{\text{def}}{=} P \ .$$

K

P

$_0 = \ . \ _1$

$_n = \ . \ _{n+1} + \ . \ _{n-1} \quad (n > 0) \ .$

n $_n$ n

!

$P \xrightarrow{\alpha} Q$

P, Q

$$\frac{}{\alpha.P \xrightarrow{\alpha} P}$$

axiom *premises*

$\alpha.P$

$\alpha.P \xrightarrow{\alpha} P$ *conclusion*

$\alpha.P$ $\alpha.P \xrightarrow{\alpha} P$

α Act a L

$$\frac{P \xrightarrow{\alpha} P}{K \xrightarrow{\alpha} P} K = P \qquad \frac{}{\alpha.P \xrightarrow{\alpha} P} \qquad \frac{P_j \xrightarrow{\alpha} P_j}{{}_{i\ I} P_i \xrightarrow{\alpha} P_j} j \quad I$$

$$\frac{P \xrightarrow{\alpha} P}{P \mid Q \xrightarrow{\alpha} P \mid Q} \qquad \frac{Q \xrightarrow{\alpha} Q}{P \mid Q \xrightarrow{\alpha} P \mid Q} \qquad \frac{P \xrightarrow{a} P \quad Q \xrightarrow{\bar{a}} Q}{P \mid Q \xrightarrow{\tau} P \mid Q}$$

$$\frac{P \xrightarrow{\alpha} P}{P[f] \xrightarrow{f(\alpha)} P[f]} \qquad \frac{P \xrightarrow{\alpha} P}{P \setminus L \xrightarrow{\alpha} P \setminus L} \alpha, \bar{\alpha} \quad L$$

$$\frac{P \xrightarrow{\alpha} P}{K \xrightarrow{\alpha} P} \quad K = P$$

K

K P

$P \xrightarrow{\alpha} P$

$\rightarrow$ . . ,

side condition $K = P$

$$\frac{P \xrightarrow{\alpha} P}{P \setminus L \xrightarrow{\alpha} P \setminus L} \quad \alpha, \bar{\alpha} \quad L$$

P

$P \setminus L$

L

$$\to \quad | \quad .\mathbf{0} \;.$$

$$.\mathbf{0} \;\to\; \mathbf{0}$$

$$| \quad .\mathbf{0} \;\to\; |\,\mathbf{0} \;.$$

$$|\,\mathbf{0}$$

0

$$| \quad .\mathbf{0} \to (\; | \quad .\mathbf{0})\,| \quad .\mathbf{0}$$

Exercise 4.7

1. [1]

$$
\begin{aligned}
{}_1 &= (\quad | \quad) \setminus \{p, v\} \\
&= \bar{p}. \quad . \quad .\bar{v}. \\
&= p.v. \quad .
\end{aligned}
$$

2. [2]

$$ {}_2 = ((\quad | \quad) | \quad) \setminus \{p, v\} $$

.

$$ = \bar{p}. \quad .\bar{v}. \quad . \quad ? $$

3.

$$ = ((\quad | \quad) \, | \quad) \setminus \{p, v\} $$

,

$$ = \bar{p}. \quad .(\quad .\bar{v}. \quad + \quad .\bar{v}.\mathbf{0}) $$

[2]

4.2.3 Value Passing CCS

pure CCS

value passing CCS

-

-

$$= \quad (x). \quad (x)$$
$$(x) \quad = \quad \overline{}(x+1). \quad .$$

x

(x)

n x (n)

n (n)

x

$\overline{}(x+1)$

$$\frac{}{a(x).P \overset{a(n)}{\rightarrow} P[n/x]} \quad n \geq 0$$

$P[n/x]$

x P n

$$\frac{}{\bar{a}(e).P \overset{\bar{a}(n)}{\rightarrow} P} \quad n$$ e

$(x_1, \ldots, x_n)$

$n \geq 0$ $x_1, \ldots, x_n$

$$\frac{P[v_1/x_1,\ldots,v_n/x_n] \xrightarrow{\alpha} P}{(e_1,\ldots,e_n) \xrightarrow{\alpha} P} \qquad (x_1,\ldots,x_n) = P \qquad e_i \qquad v_i$$

y

$a(y)$ $(x_1,\ldots,x_n)$ $y = x_i$
$1 \leq i \leq n$

$$a(x).\bar{b}(y+1).\mathbf{0}$$

y

if **then** P **else** Q

$$\begin{aligned} &= (x). \quad (x) \\ (x) &= \textbf{if } x = 0 \textbf{ then } \overline{}(0). \quad \textbf{else } \overline{}(x-1). \quad . \end{aligned}$$

(0) 0 $(n+1)$
n n
if **then** P **else** Q

$$\frac{P \xrightarrow{\alpha} P}{\textbf{if} \quad \textbf{then } P \textbf{ else } Q \xrightarrow{\alpha} P}$$

$$\frac{Q \xrightarrow{\alpha} Q}{\textbf{if} \quad \textbf{then } P \textbf{ else } Q \xrightarrow{\alpha} Q}$$

Exercise 4.8

$$\begin{aligned} &= (x). \quad (x) \\ (x) &= \overline{}(x). \quad . \end{aligned}$$

- - . -

,

.

Exercise 4.9

$$= \quad (x).(\; (x)^\frown B) + \quad .B$$
$$(x) \quad = \quad (y).(\; (y)^\frown \; (x)) + \overline{\quad}(x).D$$
$$= \quad (x). \; (x) + \bar{e}.B \; ,$$

$\frown$

$$\frown \; = (\; [p\,/p, e\,/e, o\,/o] \mid \; [p\,/ \quad , e\,/ \quad , o\,/ \quad]) \setminus \{p\,, o\,, e\,\} \; .$$

.

Exercise 4.10 (For the theoretically minded) -

1 , . 2. .

5 Behavioural Equivalence

single language approach

implementation verification

$= \overline{\quad}.$,

Definition 5.1 X *binary relation* X $X \times X$ X R X $x\,R\,y$ (x, y) R X

- R *reflexive* $x\,R\,x$ x X
- R *symmetric* $x\,R\,y$ $y\,R\,x$ x, y X
- R *transitive* $x\,R\,y$ $y\,R\,z$ $x\,R\,z$ x, y, z X

pre-order

Exercise 5.1 -

- $I = \{(n, n) \mid n \quad\}.$
- $U = \{(n, m) \mid n, m \quad\}.$
- $\leq$.
- $M_2 = \{(n, m) \mid n, m \quad, n \mod 2 = m \mod 2\}.$

R

$_i$ $0 \leq i \leq n$

$$= \quad _0\, R \quad _1\, R \quad _2\, R \cdots R \quad _n = \quad .$$

R

R

R

R

R

congruence

R

$P\, R\, Q$ $C[\,]$

$$C[P]\, R\, C[Q] \; .$$

!

5.1 Trace Equivalence: A First Attempt

trace P $\alpha_1 \cdots \alpha_k$ Act $k \geq 0$

$$P = P_0 \stackrel{\alpha_1}{\to} P_1 \stackrel{\alpha_2}{\to} \cdots \stackrel{\alpha_k}{\to} P_k \; ,$$

$P_1, \ldots, P_k$ $Traces(P)$ P
$Traces(P)$
P

P Q
P Q $Traces(P) = Traces(Q)$.

$$= \quad .\overline{\qquad}. \quad + \quad .\overline{\quad}. \quad .$$

!

$$= \overline{\quad}. \quad . \quad .$$

$$(\quad | \quad) \setminus \{ \quad , \quad , \quad \}$$

$$(\quad | \quad) \setminus \{ \quad , \quad , \quad \}$$

τ

$$(\quad | \quad) \setminus \{ \quad , \quad , \quad \} \stackrel{\tau}{\to} (\quad . \quad | \overline{\quad}. \quad) \setminus \{ \quad , \quad , \quad \} \ .$$

$$\alpha.(P + Q) = \alpha.P + \alpha.Q \ ,$$

Exercise 5.2 *completed trace* P $\alpha_1 \cdots \alpha_k$ Act *(*$k \geq 0$*)*

$$P = P_0 \stackrel{\alpha_1}{\to} P_1 \stackrel{\alpha_2}{\to} \cdots \stackrel{\alpha_k}{\to} P_k \not\to \ ,$$

$P_1, \ldots, P_k$.

,

.

1.

$$(\quad | \quad) \setminus \{ \quad , \quad , \quad \}$$

$$(\quad | \quad) \setminus \{ \quad , \quad , \quad \}$$

2. P Q -
L , $P \setminus L$ $Q \setminus L$

5.2 Strong Bisimilarity

strong bisimulation

does matter

not

De inition 5.2 R

bisimulation s_1 R s_2 α

$s_1 \overset{\alpha}{\to} s_1$ $s_2 \overset{\alpha}{\to} s_2$ s_1 R s_2

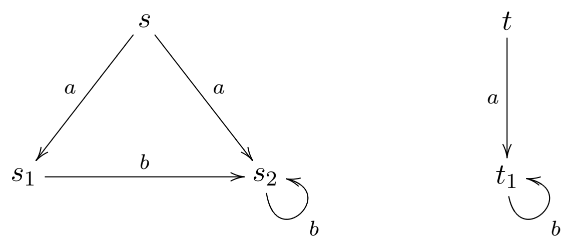
$s_2 \overset{\alpha}{\to} s_2$ $s_1 \overset{\alpha}{\to} s_1$ s_1 R s_2

s s *bisimilar* s s

strong bisimulation *equivalence* *strong bisimilarity*

Example 5.1 $(\mathsf{Proc}, \mathsf{Act}, \{\overset{a}{\to} \mid a \quad \mathsf{Act}\})$

- $\mathsf{Proc} = \{s, s_1, s_2, t, t_1\}$
- $\mathsf{Act} = \{a, b\}$
- $\overset{a}{\to} = \{(s, s_1), (s, s_2), (t, t_1)\}$
- $\overset{b}{\to} = \{(s_1, s_2), (s_2, s_2), (t_1, t_1)\}$

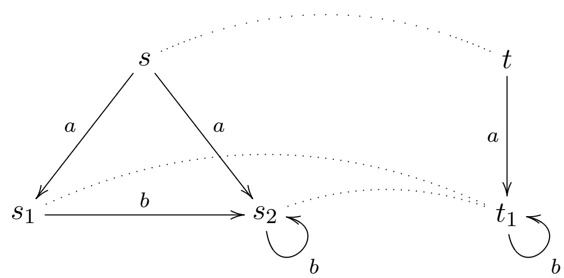


s t

R (s,t) R

$$R = \{(s,t),(s_1,t_1),(s_2,t_1)\} \ .$$

R



(s,t) R R

R

a

a

R

- (s,t)
  - s

    $s \xrightarrow{a} s_1$ $t \xrightarrow{a} t_1$ (s_1,t_1) R

    $s \xrightarrow{a} s_2$ $t \xrightarrow{a} t_1$ (s_2,t_1) R

    s
  - t

    $t \xrightarrow{a} t_1$ $s \xrightarrow{a} s_2$ (s_2,t_1) R

    $s \xrightarrow{a} s_1$

t

- (s_1, t_1)
  - s_1

    $s_1 \xrightarrow{b} s_2$ $t_1 \xrightarrow{b} t_1$ (s_2, t_1) *R*

    s_1
  - t_1

    $t_1 \xrightarrow{b} t_1$ $s_1 \xrightarrow{b} s_2$ (s_2, t_1) *R*

    t_1
- (s_2, t_1)
  - s_2

    $s_2 \xrightarrow{b} s_2$ $t_1 \xrightarrow{b} t_1$ (s_2, t_1) *R*

    s_2
  - t_1

    $t_1 \xrightarrow{b} t_1$ $s_2 \xrightarrow{b} s_2$ (s_2, t_1) *R*

    t_1

R (s, t) *R*
s t

s_1 s_2

$$R = \{(s_1, s_2), (s_2, s_2)\} \ .$$

R

Example 5.2

$(\mathrm{Proc}, \mathrm{Act}, \{\xrightarrow{a} \mid a \quad \mathrm{Act}\})$

- Proc $= \{s_i \mid i \quad \mathbb{N}\} \quad \{t\}$ $\quad \mathbb{N} = \{1, 2, 3, \ldots\}$
- Act $= \{a\}$
- $\xrightarrow{a} = \{(s_i, s_{i+1}) \mid i \quad \mathbb{N}\} \quad \{(t, t)\}$

$$s_1 \xrightarrow{a} s_2 \xrightarrow{a} s_3 \xrightarrow{a} s_4 \xrightarrow{a} \cdots$$

$$\begin{tikzcd} t \arrow[loop right, "a"] \end{tikzcd}$$

s_1 t

$$R = \{(s_i, t) \mid i \quad \mathbb{N}\}$$

(s_1, t)

not

R

R .

$\rightarrow \overline{}.$.

$\rightarrow P$

P P R $\overline{}.$

$\overline{}.$ $+ \overline{}.$

$\overline{}.$ $+ \overline{}.$ R $\overline{}.$.

$\overline{}.$ $+ \overline{}.$ $\overline{\rightarrow}$,

$\overline{}.$

Example 5.3 P Q

$$
\begin{aligned}
P &= a.P_1 + b.P_2 \\
P_1 &= c.P \\
P_2 &= c.P
\end{aligned}
$$

$$
\begin{aligned}
Q &= a.Q_1 + b.Q_2 \\
Q_1 &= c.Q_3 \\
Q_2 &= c.Q_3 \\
Q_3 &= a.Q_1 + b.Q_2 \ .
\end{aligned}
$$

P Q

$$\mathsf{R} = \{(P,Q),(P,Q_3),(P_1,Q_1),(P_2,Q_2)\} \ .$$

Exercise 5.3 P Q

$$
\begin{aligned}
P &= a.P_1 \\
P_1 &= b.P + c.P
\end{aligned}
$$

$$
\begin{aligned}
Q &= a.Q_1 \\
Q_1 &= b.Q_2 + c.Q \\
Q_2 &= a.Q_3 \\
Q_3 &= b.Q + c.Q_2 \ .
\end{aligned}
$$

P Q .

Exercise 5.4

$$
\begin{aligned}
P &= a.(b.\mathbf{0} + c.\mathbf{0}) \\
Q &= a.b.\mathbf{0} + a.c.\mathbf{0} \ .
\end{aligned}
$$

P Q *not* .

Theorem 5.1

s_1 s_2 α

$s_1 \overset{\alpha}{\to} s_1$ $s_2 \overset{\alpha}{\to} s_2$ s_1 s_2

$s_2 \overset{\alpha}{\to} s_2$ $s_1 \overset{\alpha}{\to} s_1$ s_1 s_2

Proof: $(\mathsf{Proc}, \mathsf{Act}, \{\overset{\alpha}{\to} \mid \alpha \quad \mathsf{Act}\})$

Proc

s_1 s_2 s_2 s_3 s_1 s_2 s_3 Proc
s_1 s_3 s_1 s_2
s_2 s_3 *R* *R*
(s_1, s_2) (s_2, s_3)

$$S = \{(s_1, s_3) \mid (s_1, s_2) \quad R \qquad (s_2, s_3) \quad R, \qquad s_2\} .$$

(s_1, s_3) *S* *R*
R *S*
s_1 s_3

Proc

$$= \square \{R \mid R \qquad \} .$$

$$(s_1, s_2) \quad \square \{R \mid R \qquad \} \quad s_1 \xrightarrow{\alpha} s_1 ,$$

s_2 $s_2 \xrightarrow{\alpha} s_2$

$$(s_1, s_2) \quad \square \{R \mid R \qquad \} .$$

$$(s_1, s_2) \quad \square \{R \mid R \qquad \} ,$$

R (s_1, s_2) *R*
$s_1 \xrightarrow{\alpha} s_1$ s_2 $s_2 \xrightarrow{\alpha} s_2$
(s_1, s_2) *R* (s_1, s_2)

$$\square \{R \mid R \qquad \} .$$

s_2 $s_2 \xrightarrow{\alpha} s_2$

$$(s_1, s_2) \quad \{R \mid R \qquad \} ,$$

s_1 s_2 α

$s_1 \xrightarrow{\alpha} s_1$ $s_2 \xrightarrow{\alpha} s_2$ s_1 s_2

$s_2 \xrightarrow{\alpha} s_2$ $s_1 \xrightarrow{\alpha} s_1$ s_1 s_2

s_1 s_2

Proc

α

$s_1 \xrightarrow{\alpha} s_1$ $s_2 \xrightarrow{\alpha} s_2$

s_1 s_2

$s_2 \xrightarrow{\alpha} s_2$ $s_1 \xrightarrow{\alpha} s_1$

s_1 s_2

s_1 s_2

(s_1, s_2)

R

(s_1, s_2) R s_1 s_2 R

$s_1 \xrightarrow{\alpha} s_1$ s_1

$s_2 \xrightarrow{\alpha} s_2$ s_2 s_2 (s_1, s_2) R

R !

R

$$\mathsf{R} = \{(s_1, s_2)\} \quad .$$

(s_1, s_2) R

R

s_1 s_2

$\square$

Exercise 5.5 *.1*

.

Exercise 5.6 K $K = P$.
K P .

Exercise 5.7 ,
-
(10).
$\alpha_1 \cdots \alpha_k$ ($k \geq 0$)

P Q $\alpha_1 \cdots \alpha_k$ $Traces(P)$ $\alpha_1 \cdots \alpha_k$ $Traces(Q)$.

Exercise 5.8

$\{(P \mid Q, Q \mid P) \mid$ P, Q $\}$
$\{(P \mid \mathbf{0}, P) \mid$ P $\}$
$\{((P \mid Q) \mid R, P \mid (Q \mid R)) \mid$ P, Q, R $\}$.

, $P, Q, R,$

$$P \mid Q \qquad Q \mid P$$
$$P \mid \mathbf{0} \qquad P$$
$$(P \mid Q) \mid R \qquad P \mid (Q \mid R) \ .$$

$\Pi_{i=1}^{k} P_i$ $k \geq 0$
P_i

$$P_1 \mid P_2 \mid \cdots \mid P_k \ .$$

$k = 0$ $\mathbf{0}$

Proposition 5.1 P, Q, R P Q

- $\alpha.P$ $\alpha.Q$ α
- $P + R$ $Q + R$ $R + P$ $R + Q$ R
- $P \mid R$ $Q \mid R$ $R \mid P$ $R \mid Q$ R
- $P[f]$ $Q[f]$ f
- $P \setminus L$ $Q \setminus L$ L

Proof:

P Q

- R $P \mid R$ $Q \mid R$ $\mathcal{R}$ $(P \mid R, Q \mid R)$

$$\mathcal{R} = \{(P \mid R, Q \mid R) \mid P \quad Q \quad P, Q, R \quad\} \ .$$

$(P \mid R, Q \mid R)$ $\mathcal{R}$ $\mathcal{R}$ $\mathcal{R}$

$\mathcal{R}$ $(P \mid R, Q \mid R)$ $\mathcal{R}$ $P \mid R \xrightarrow{\alpha} S$ α S $Q \mid R \xrightarrow{\alpha} T$ T (S, T) $\mathcal{R}$ $(P \mid R, Q \mid R)$ $\mathcal{R}$ $P \mid R \xrightarrow{\alpha} S$ α S $P \mid R \xrightarrow{\alpha} S$

$P \mid R \xrightarrow{\alpha} S$

P R $P \mid R \xrightarrow{\alpha} S$ $P \xrightarrow{\alpha} P$ $S = P \mid R$ P

R P $P \mid R \xrightarrow{\alpha} S$ $R \xrightarrow{\alpha} R$ $S = P \mid R$ R

P R $P \mid R \xrightarrow{\alpha} S$ $\alpha = \tau$ $P \xrightarrow{a} P$

$$Q \mid R \xrightarrow{\alpha} Q \mid R .$$

$\mathcal{R}$

$$(P \mid R, Q \mid R) \quad \mathcal{R} .$$

$T = Q \mid R$

$R \xrightarrow{\alpha} R$

$$Q \mid R \xrightarrow{\alpha} Q \mid R .$$

$\mathcal{R}$

$$(P \mid R, Q \mid R) \quad \mathcal{R} .$$

$T = Q \mid R$

$P \xrightarrow{a} P$ P Q $Q \xrightarrow{a} Q$ P Q

Q $Q \xrightarrow{a} Q$ $R \xrightarrow{\bar{a}} R$

$$Q \mid R \xrightarrow{\tau} Q \mid R .$$

$\mathcal{R}$

$$(P \mid R, Q \mid R) \quad \mathcal{R} .$$

$T = Q \mid R$

$\mathcal{R}$

- L $P \setminus L$ $Q \setminus L$ $\mathcal{R}$ $(P \setminus L, Q \setminus L)$

$$\mathcal{R} = \{(P \setminus L, Q \setminus L) \mid P \quad Q\} .$$

$(P \setminus L, Q \setminus L)$ $\mathcal{R}$

– R

– $(P \setminus L, Q \setminus L)$ R $P \setminus L \xrightarrow{\alpha} S$
α S $Q \setminus L \xrightarrow{\alpha} T$ T
(S,T) R

□

Exercise 5.9 , -
.

Exercise 5.10 L $P,$
$\tau_L(P)$ τ α P
α L $\bar{\alpha}$ $L.$, $\tau_L(\ )$

$$\frac{P \xrightarrow{\alpha} P}{\tau_L(P) \xrightarrow{\tau} \tau_L(P\ )} \quad \alpha \quad L \quad \bar{\alpha} \quad L$$

$$\frac{P \xrightarrow{\mu} P}{\tau_L(P) \xrightarrow{\mu} \tau_L(P\ )} \quad \mu = \tau \quad \mu, \bar{\mu} \quad L$$

$\tau_L(P)$ $\tau_L(Q),$ P $Q.$
$\tau_L(\ )$
, $C_L[\ ]$ (
) , $P,$

$\tau_L(P)$ $C_L[P]$

$$_0 = \ . \quad _1$$

$$_n = \ . \quad _{n+1} + \quad . \quad _{n-1} \quad (n > 0) \ .$$

$$= \ .(\ | \quad .\mathbf{0}) \ .$$

$_0$
R

$\{(C \mid \Pi_{i=0}^{k} P_i, \quad _n) \mid$ (1) $k \geq 0$,
(2) $P_i = \mathbf{0}$ $P_i =$ $.\mathbf{0},$ i ,
(3) i $P_i =$ $.\mathbf{0}$ $n\}$

Proposition 5.2 R

Proof:

$C \mid \Pi_{i=1}^{k} P_i \; R \; {}_n$.

R P_i $\mathbf{0}$ $.\mathbf{0}$

$P_i =$ $.\mathbf{0}$ n

$C \mid \Pi_{i=1}^{k} P_i \xrightarrow{\alpha} P$ α P

Q ${}_n \xrightarrow{\alpha} Q$ $P \; R \; Q$

${}_n \xrightarrow{\alpha} Q$ α Q

P $C \mid \Pi_{i=1}^{k} P_i \xrightarrow{\alpha} P$ $P \; R \; Q$

$C \mid \Pi_{i=1}^{k} P_i \xrightarrow{\alpha} P$ α P

- $\alpha =$ $P = C \mid$ $.\mathbf{0} \mid \Pi_{i=1}^{k} P_i$
- $n > 0$ $\alpha =$ $P = C \mid \Pi_{i=1}^{k} P_i$ $(P_1, \ldots, P_k)$ $(P_1, \ldots, P_k)$ ℓ $P_\ell =$ $.\mathbf{0}$ $P_\ell = \mathbf{0}$

$${}_n \rightarrow \quad {}_{n+1} \; .$$

$${}_n \rightarrow \quad {}_{n-1} \; .$$

${}_n \xrightarrow{\alpha} Q$ α Q

- $\alpha =$ $Q =$ ${}_{n+1}$
- $n > 0$ $\alpha =$ $Q =$ ${}_{n-1}$

$C \mid \Pi_{i=1}^{k} P_i$

□

Exercise 5.11 .

Exercise 5.12 (Simulation) $\mathcal{R}$
simulation $s_1 \mathcal{R} s_2$ α

- $s_1 \xrightarrow{\alpha} s_1$, $s_2 \xrightarrow{\alpha} s_2$ $s_1 \mathcal{R} s_2$.

s *simulates* s, $s \sqsubseteq\!\!\!\!\!\sim s$, $\mathcal{R}$ $s \mathcal{R} s$.
s s *simulation equivalent,* s s , $s \sqsubseteq\!\!\!\!\!\sim s$ $s \sqsubseteq\!\!\!\!\!\sim s$
.

1. $\sqsubseteq\!\!\!\!\!\sim$.

2.

$$
\begin{aligned}
a.\mathbf{0} &\;\sqsubseteq\!\!\!\!\!\sim\; a.a.\mathbf{0} \\
a.b.\mathbf{0} + a.c.\mathbf{0} &\;\sqsubseteq\!\!\!\!\!\sim\; a.(b.\mathbf{0} + c.\mathbf{0}) \;\; .
\end{aligned}
$$

3. .

Exercise 5.13 (For the theoretically minded)

$$
\begin{aligned}
P &= a.b.c.\mathbf{0} + a.b.d.\mathbf{0} \\
Q &= a.(b.c.\mathbf{0} + b.d.\mathbf{0}) \;\; .
\end{aligned}
$$

, , P Q .

1. P Q (.2)

2. R L,

$$(P \mid R) \setminus L \qquad (Q \mid R) \setminus L$$

.

P Q ,
.

.

5.3 Weak Bisimilarity

$$\begin{array}{rl} P \mid Q & Q \mid P \\ P \mid \mathbf{0} & P \\ (P \mid Q) \mid R & P \mid (Q \mid R)\ . \end{array}$$

τ
internal *unobservable*
τ

τ

$a.\tau.\mathbf{0}$ $a.\mathbf{0}$ τ

$a.\tau.\mathbf{0}$ $a.\mathbf{0}$ *not*
each
one
τ $a.\tau.\mathbf{0}$
$a\tau$ $a.\mathbf{0}$

τ

$\downarrow \overline{}$

$(\quad _b \mid \quad) \setminus \{ \quad , \quad \}$

$\tau \qquad \tau$

$\tau \downarrow$

$$
\begin{aligned}
&= (\quad _b \mid \quad) \setminus \{ \quad , \quad \} && = \overline{}. \\
&= (\overline{} . \quad _b \mid \quad) \setminus \{ \quad , \quad \} && = \overline{}. \\
&= (\quad _b \mid \quad) \setminus \{ \quad , \quad \} && = \quad . \quad .
\end{aligned}
$$

$(\quad _b \mid \quad) \setminus \{ \quad , \quad \}$

τ

τ

τ

$a.\tau.\mathbf{0} \qquad a.\mathbf{0}$

τ

$$_b = \quad . \overline{} . \quad _b + \quad . \quad _b \, .$$

b

$(\quad _b \mid \quad) \setminus \{ \quad , \quad \} \qquad \tau$

$(\quad _b \mid \quad) \setminus \{ \quad , \quad \}$

$$(\quad _b \mid \quad) \setminus \{ \quad , \quad \} \xrightarrow{\tau} (\quad _b \mid \quad) \setminus \{ \quad , \quad \} \, ,$$

f ϵ *not*

not

$(\quad {}_b \,|\quad) \setminus \{\quad ,\quad \}$

$(\quad {}_b \,|\quad) \setminus \{\quad ,\quad \}$

De inition 5.3 P Q $P \;{}^{\epsilon}\; Q$
τ P Q
$P = Q$
α $P \;{}^{\alpha}\; Q$ P Q

$$P \;{}^{\epsilon}\; P \overset{\alpha}{\to} Q \;{}^{\epsilon}\; Q\ .$$

α $\hat{\alpha}$ ϵ $\alpha = \tau$ α

$P \;{}^{\alpha}\; Q$ P Q α
τ
$a.\tau.\mathbf{0} \;{}^{a}\; \mathbf{0}$ $a.\tau.\mathbf{0} \;{}^{a}\; \tau.\mathbf{0}$

.

De inition 5.4
R *weak bisimulation* $s_1 \; R \; s_2$
α

$s_1 \xrightarrow{\alpha} s_1$ $s_2 \; \hat{\alpha} \; s_2$ $s_1 \; R \; s_2$

$s_2 \xrightarrow{\alpha} s_2$ $s_1 \; \hat{\alpha} \; s_1$ $s_1 \; R \; s_2$

s s *observationally equivalent* *weakly bisimilar*
$s \approx s$
$\approx$ *observational equivalence* *weak bisimilarity*

Example 5.4

$$s \xrightarrow{\tau} s_1 \xrightarrow{a} s_2 \qquad t \xrightarrow{a} t_1$$

s t $s \approx t$

$$R = \{(s,t), (s_1,t), (s_2,t_1)\}$$

(s,t) R R

- (s,t)
  $s \xrightarrow{\tau} s_1$ $t \; \varepsilon \; t$ (s_1,t) R $t \xrightarrow{a} t_1$ $s \; a \; s_2$ (s_2,t_1) R
- (s_1,t) $s_1 \xrightarrow{a} s_2$ $t \; a \; t_1$
  (s_2,t_1) R $t \xrightarrow{a} t_1$ $s_1 \; a \; s_2$ (s_2,t_1) R
- (s_2,t_1) s_2 t_1
  R

R
R

$$a.\mathbf{0} \approx a.\tau.\mathbf{0}$$

$= \overline{}.$,

Exercise 5.14 .

Exercise 5.15 .
.

$$
\begin{aligned}
&= a.\mathbf{0} + \tau. \\
&= b.\mathbf{0} + \tau. \quad .
\end{aligned}
$$

a b

$$\approx \quad \approx a.\mathbf{0} + b.\mathbf{0} \; .$$

!

$a.\mathbf{0} + b.\mathbf{0}$ *not*

$\mathbf{0}$

$$= \tau. \quad .$$

$$
\begin{aligned}
&= \quad . && = \quad . \\
&= \overline{\quad\quad} . && = \overline{\quad} . \\
&= \quad . \quad + \quad . && = \overline{\quad} .
\end{aligned}
$$

$$
\begin{aligned}
&= \quad . \\
&= \tau. \quad + \overline{\quad\quad} . \\
&= \overline{\quad\quad} .
\end{aligned}
$$

$$(\quad | \quad | \quad) \setminus L \qquad (L = \{ \quad , \quad , \quad , \quad \})$$

Exercise 5.16 .

Theorem 5.2 $\approx$

$s_1 \approx s_2$ α

$s_1 \stackrel{\alpha}{\to} s_1$ s_2 $\hat{\alpha}$ s_2 $s_1 \approx s_2$

$s_2 \stackrel{\alpha}{\to} s_2$ s_1 $\hat{\alpha}$ s_1 $s_1 \approx s_2$

Proof:
□

Exercise 5.17 .

Exercise 5.18 -
.

Exercise 5.19 , P, Q, ,
Milner's τ-laws,

$$
\begin{aligned}
\alpha.\tau.P &\approx \alpha.P \\
P + \tau.P &\approx \tau.P \\
\alpha.(P + \tau.Q) &\approx \alpha.(P + \tau.Q) + \alpha.Q \ .
\end{aligned}
$$

Exercise 5.20 , P, Q, P ϵ Q Q ϵ P, $P \approx Q$.

Exercise 5.21 *τ-free*
τ- .
, $a.\mathbf{0}$ τ- , $a.(b.\mathbf{0} \mid \bar{b}.\mathbf{0})$.
τ- $a.\mathbf{0} + \tau.\mathbf{0}$.

Exercise 5.22 , P, $P \setminus (\mathsf{Act} - \{\tau\})$
$\mathbf{0}$.

not
not

$\mathbf{0}$ $\tau.\mathbf{0}$

$$a.\mathbf{0} + \mathbf{0} \approx a.\mathbf{0} \approx a.\mathbf{0} + \tau.\mathbf{0} \ .$$

$a.\mathbf{0} + \tau.\mathbf{0} \xrightarrow{\tau} \mathbf{0}$ $a.\mathbf{0} + \mathbf{0} \ {}^{\epsilon} \ a.\mathbf{0} + \mathbf{0}$
$\mathbf{0}$ $a.\mathbf{0} + \mathbf{0}$

Proposition 5.3 P, Q, R $P \approx Q$

- $\alpha.P \approx \alpha.Q$ α
- $P \mid R \approx Q \mid R$ $R \mid P$ $R \mid Q$ R
- $P[f] \approx Q[f]$ f
- $P \setminus L \approx Q \setminus L$ L

Proof:

□

Exercise 5.23 .3.

5.4 Game Characterizations of Strong and Weak Bisimilarity

What techniques do we have to show that two states are not bisimilar?

s t s t

(s, t)

2^{25}

n

2^{n^2}

'attacker'

'defender'

De inition 5.5 $(\mathsf{Proc}, \mathsf{Act}, \{\xrightarrow{a} \mid a \quad \mathsf{Act}\})$

strong bisimulation game

(s_1, t_1) Proc × Proc *'attacker'*

'defender'

rounds

Proc × Proc *current*

(s_1, t_1)

(s, t)

(s, t) a Act

- $s \xrightarrow{a} s$ s Proc
- $t \xrightarrow{a} t$ t Proc

- $t \xrightarrow{a} t$ t Proc
- $s \xrightarrow{a} s$ s Proc

$(s\ , t\ )$

play

(s_1, t_1)

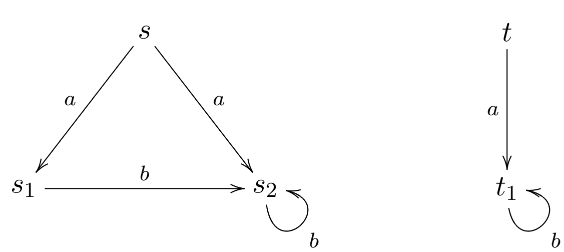
(s, t)

$s \nrightarrow$ $t \nrightarrow$

Proposition 5.4 s_1 t_1

(s_1, t_1) s_1 t_1

Example 5.5



(s, t) s t

(s, t)

a $t \xrightarrow{a} t_1$

a $s \xrightarrow{a} s_2$

a $s \xrightarrow{a} s_1$

- $s \xrightarrow{a} s_2$

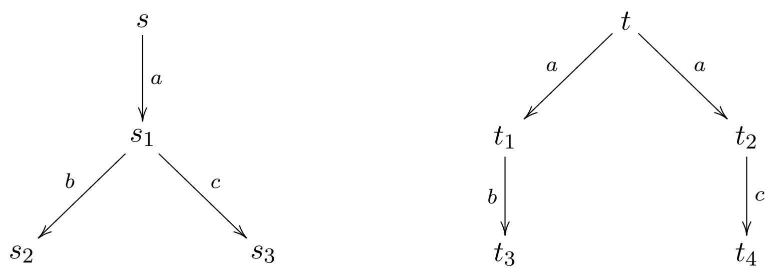
  (s_2, t_1)
- $t \xrightarrow{a} t_1$
  (s_2, t_1)
- $t \xrightarrow{a} t_1$
  (s_1, t_1)

(s_2, t_1) (s_1, t_1)
(s_2, t_1)
(s_2, t_1)

(s_1, t_1) $s_1 \xrightarrow{b} s_2$ $t_1 \xrightarrow{b} t_1$
$t_1 \xrightarrow{b} t_1$ $s_1 \xrightarrow{b}$
s_2 (s_2, t_1)

(s, t) s t

Example 5.6



s t

(s, t)

- a
  $s \xrightarrow{a} s_1$ $t \xrightarrow{a} t_1$ $t \xrightarrow{a} t_2$

  (s_1, t_1) (s_1, t_2) (s_1, t_1) $s_1 \xrightarrow{c} s_3$

  c

  t_1 (s_1, t_2) $s_1 \xrightarrow{b} s_2$

  t_2

  s t

- (s, t)

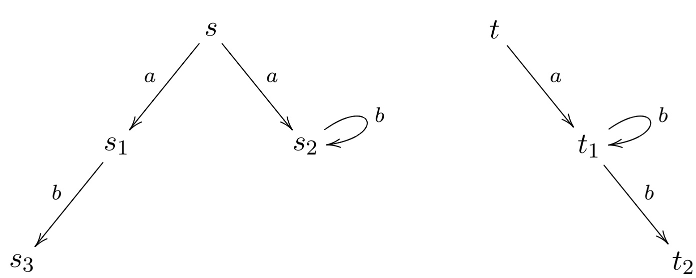
  $t \xrightarrow{a} t_1$

  $s \xrightarrow{a} s_1$

  (s_1, t_1) $s_1 \xrightarrow{c} s_3$

  $t_1 \overset{c}{\not\rightarrow}$

Example 5.7



(s, t)

s t

$s \xrightarrow{a} s_1$

$t \xrightarrow{a} t_1$ (s_1, t_1)

$t_1 \xrightarrow{b} t_1$ $s_1 \xrightarrow{b} s_3$

(s_3, t_1) $t_1 \xrightarrow{b} t_1$

$t_1 \xrightarrow{b} t_2$ $s_3 \nrightarrow$

5.4.1 Weak Bisimulation Games

τ

not

Definition 5.6 *weak bisimulation game*

$\hat{\alpha}$

$\xrightarrow{a}$ $\xrightarrow{a}$

Proposition 5.5 s_1 t_1

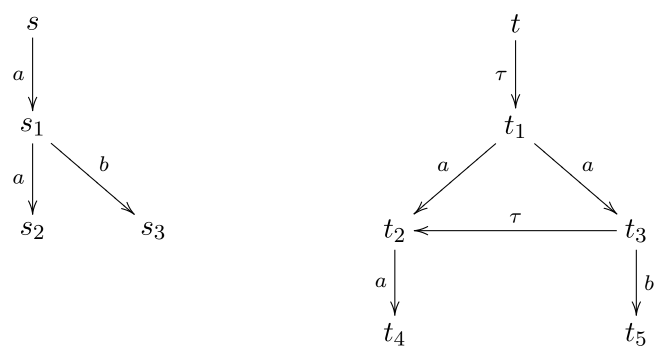
(s_1, t_1) s_1 t_1

(s, t)

τ $s \xrightarrow{\tau} s$

t $t \stackrel{\varepsilon}{} t$

Example 5.8



$s \approx t$

(s, t)

a

$s \xrightarrow{a} s_1$ t ^{a} t_2

t_1 t ^{a} t_2 t_1 t_3 t ^{a} t_3 t_1

(s_1, t_2) (s_1, t_3)

(s_1, t_2) $s_1 \xrightarrow{b} s_3$

$t_2 \overset{b}{\not\Rightarrow}$

(s_1, t_3) τ

!

a

-
-
-
-
-

our computer scientist is willing to drink both coffee and tea now?

1

Hennessy-Milner logic

De inition 6.1 Act

M

$$F ::= tt \mid ff \mid F \quad G \mid F \quad G \mid \; a \; F \mid [a]F$$

a Act $A = \{a_1, \ldots, a_n\}$ Act $n \geq 0$ A F
a_1 F $\ldots$ a_n F $[A]F$ $[a_1]F$ $\ldots$ $[a_n]F$
$A =$ A $F = ff$ $[A]F = tt$

Act

M

- tt
- ff
- F G F G F G F G
- a F a Act a F
- $[a]F$ a Act a F

a F *possible* a F $[a]F$ a *necessarily* F *possibly* *necessarily* *modal logics*

$$(\mathsf{Proc}, \mathsf{Act}, \{ \xrightarrow{a} \mid a \quad \mathsf{Act}\}) \ .$$

$[\![F]\!]$ Proc F

De inition 6.2 $[\![F]\!]$ Proc F M

1. $[\![tt]\!] = \mathsf{Proc}$,
2. $[\![ff]\!] =$
3. $[\![F \quad G]\!] = [\![F]\!] \cap [\![G]\!]$,
4. $[\![F \quad G]\!] = [\![F]\!] \quad [\![G]\!]$,
5. $[\![\ a \ F]\!] = \ \cdot a \cdot \ [\![F]\!]$,
6. $[\![[a]F]\!] = [\cdot a \cdot][\![F]\!]$,

$$\cdot a \cdot \ , [\cdot a \cdot] : P(\mathsf{Proc}) \to P(\mathsf{Proc})$$

$$\begin{aligned} \cdot a \cdot \ S &= \{p \quad \mathsf{Proc} \mid \ p \ . \ p \xrightarrow{a} p \qquad p \quad S\} \\ [\cdot a \cdot]S &= \{p \quad \mathsf{Proc} \mid \ p \ . \ p \xrightarrow{a} p \ = \quad p \quad S\}. \end{aligned}$$

$p \models F \quad p \quad [\![F]\!]$

equivalent

M

$\xrightarrow{a}$

τ P a

$P \xrightarrow{a} Q$

Q

F F

F

$F = tt$

tt

$$
\begin{aligned}
[\![\quad tt]\!] &= \cdot \quad \cdot [\![tt]\!] \\
&= \cdot \quad \cdot \mathsf{Proc} \\
&= \{P \mid P \to P \quad P \quad \mathsf{Proc}\} .
\end{aligned}
$$

$[\quad]ff$

ff

$[\quad]ff$

$$
\begin{aligned}
[\![[\quad]ff]\!] &= [\cdot \quad \cdot][\![ff]\!] \\
&= [\cdot \quad \cdot] \\
&= \{P \mid \quad P . P \to P \;=\; P \quad\} \\
&= \{P \mid P \not\to\} .
\end{aligned}
$$

P

$$P \not\to \quad (\; P . P \to P \;=\; P \quad) .$$

$P \to Q$ Q

P P $P \to P$ Q

$P \not\to$

P P $P \to P$ P

!

not a Act

$[a]ff$

$$[\quad] \quad tt .$$

Exercise 6.1

1.

.

2.

-
- ,
-

.

3. a ff $[a]tt$

Exercise 6.2

$$= \quad . \quad .$$

$$[\quad](\quad tt \quad [\quad] ff) \; .$$

, $n \geq 0$,

$$\underbrace{\quad \ldots \quad}_{n\text{-}} tt \; .$$

Exercise 6.3 (Mandatory) M $a.b.\mathbf{0} + a.c.\mathbf{0}$, $a.(b.\mathbf{0} + c.\mathbf{0})$. M $a.(b.c.\mathbf{0} + b.d.\mathbf{0})$, $a.b.c.\mathbf{0} + a.b.d.\mathbf{0}$.

$\models$

$\models$

- $P \models tt$ P
- $P \models ff$ P
- $P \models F \quad G$ $P \models F$ $P \models G$
- $P \models F \quad G$ $P \models F$ $P \models G$

- $P \models \ a \ F$ $P \xrightarrow{a} P$ P $P \models F$
- $P \models [a]F$ $P \models F$ P $P \xrightarrow{a} P$

Exercise 6.4 -

.2.

.

not

M M *is*

F M F^c M

F F^c F

1. $tt^c = ff$,
2. $ff^c = tt$
3. $(F \quad G)^c = F^c \quad G^c$,
4. $(F \quad G)^c = F^c \quad G^c$,
5. $(\ a \ F)^c = [a]F^c$,
6. $([a]F)^c = \ a \ F^c$.

$$
\begin{aligned}
(\ a \ tt)^c &= [a]ff \\
([a]ff)^c &= \ a \ tt.
\end{aligned}
$$

Proposition 6.1 $(\mathsf{Proc}, \mathsf{Act}, \{\xrightarrow{a} \mid a \quad \mathsf{Act}\})$ F M $[\![F^c]\!] = \mathsf{Proc} \setminus [\![F]\!]$

Proof: F $\square$

Exercise 6.5

1. .1.

2. , , $(F^c)^c = F$ F M. F.

P

F $P \models F$ $P \models F^c$

$[\![F]\!]$ $[\![F^c]\!]$

$$= \quad a. \quad + a.\mathbf{0}$$
$$= \quad a.a. \quad + a.\mathbf{0} \quad .$$

not

$$\xrightarrow{a} \quad .$$

$$\xrightarrow{a} \mathbf{0}$$

$$\xrightarrow{a} a. \quad .$$

$\mathbf{0}$ $a.$
a $\mathbf{0}$

$$a. \quad \xrightarrow{a}$$

$a.$ $\mathbf{0}$

a a $[a]$ff a
a

!

M

M

M

De inition 6.3 P *image finite*
$\{P \mid P \xrightarrow{a} P\}$ a

$!A$

$$!A = a.\mathbf{0}|!A$$

not n

$n \geq 0$

$$!A \xrightarrow{a} \underbrace{a.\mathbf{0} \mid \cdots \mid a.\mathbf{0}}_{n} |\mathbf{0}|!A \ .$$

$$^{<\omega} = \sum_{i \geq 0} a^i \ ,$$

$a^0 = \mathbf{0}$ $a^{i+1} = a.a^i$

Theorem 6.1 $(\mathsf{Proc}, \mathsf{Act}, \{\xrightarrow{a} \mid a \ \ \mathsf{Act}\})$ P, Q Proc P Q P Q *M*

Proof:

- P Q $P \models F$ F *M* F $Q \models F$ P Q *M*

  F $F = [a]G$ a G R S R S $R \models G$ $S \models G$ $Q \models [a]G$ $Q \xrightarrow{a} Q$ Q $Q \models G$ P Q $Q \xrightarrow{a} Q$ P $P \xrightarrow{a} P$ P Q $P \models [a]G$ $P \models G$ $Q \models G$ Q $Q \xrightarrow{a} Q$ G $Q \models [a]G$

- P Q *M* P Q

$$\mathcal{R} = \{(R, S) \mid R, S \ \ \mathsf{Proc} \ \ \ \ M\}$$

$R \; \mathcal{R} \; S$ $R \xrightarrow{a} R$

S $S \xrightarrow{a} S$ $R \; \mathcal{R} \; S$

$\mathcal{R}$ $\mathcal{R}$

S $S \xrightarrow{a} S$

S R S

S a

$\{S_1, \ldots, S_n\}$ $n \geq 0$

R i $\{1, \ldots, n\}$

F_i

$$R \models F_i \qquad S_i \models F_i \ .$$

$$R \models F_i \qquad S_i \models F_i \qquad i \quad \{1, \ldots, n\}$$

R

S R S

$$a \ (F_1 \quad F_2 \quad \cdots \quad F_n)$$

R S

$\square$

Exercise 6.6 .

R S

$n = 0$

Remark 6.1

$\mathcal{M}$

Exercise 6.7 (For the Theoretically Minded) $^{\omega}$

$$^{\omega} = a. \ ^{\omega} \ .$$

$^{<\omega}$ $^{\omega} + \ ^{<\omega}$, $^{<\omega}$ (21), *1.* ,

2. M.

.1

M, . -

.

ω F M a^i, i

F.

modal depth

.

7 Hennessy-Milner Logic with Recursive Definitions

finite

modal depth

$[a]$ a ff b tt

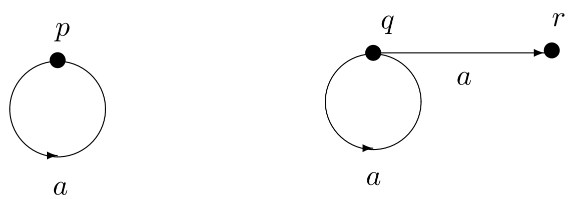
always

Example 7.1 p q

p q

a p q

$$
\begin{aligned}
p &\models [a]\ a\ tt\\
q &\models [a]\ a\ tt.
\end{aligned}
$$



q

r

$$r = r_0 \xrightarrow{a} r_1 \xrightarrow{a} r_2 \xrightarrow{a} r_3 \cdots r_{n-1} \xrightarrow{a} r_n \quad (n \geq 0).$$

n

p q

$$\begin{aligned} p &\models [a]^{n+1}\ a\ tt \\ q &\models [a]^{n+1}\ a\ tt. \end{aligned}$$

n !

p q p

a $a\ tt$

invariance $Inv(\ a\ tt)$

$$Inv(\ a\ tt) = \ a\ tt \quad [a]\ a\ tt \quad [a][a]\ a\ tt \quad \cdots = \prod_{i=0}^{\infty} [a]^i\ a\ tt.$$

a

$a\ tt$

i

i

$[a]^i\ a\ tt$

q

a r

q $[a]ff$ $Pos([a]ff)$

$$Pos([a]ff) = [a]ff \quad a \ [a]ff \quad a \quad a \ [a]ff \quad \cdots = \sum_{i=0}^{\infty} a^{\ i}[a]ff.$$

a

$[a]ff$ i

a

i $a^{\ i}[a]ff$

recursion a

$Inv(\ a \ tt)$

$$X \quad \equiv \quad a \ tt \quad [a]X,$$

$F \equiv G$ F G

$[\![F]\!] = [\![G]\!]$

a

a

a

!

$$x = x + 1$$

X

$$X = \quad \setminus X \quad .$$

$$X$$

$$X = \{2\} \quad X \ ,$$

$$2$$

$$X = \{10\} \quad \{n - 1 \mid n \quad X,\ n = 0\} \ .$$

$\{0, 1, \ldots, 10\}$

Exercise 7.1 .

-
-
-

S

$$S \ = \ \ \cdot a \cdot \ \mathsf{Proc} \cap [\cdot a \cdot]S.$$

$S =$
$a\ tt$ $[a]ff$ p
maximal
$S = \{p\}$ $S =$ *minimal solution*

$Pos([a]ff)$

$$Y \ \equiv \ [a]ff \quad a\ Y.$$

$$Y \ = \{p, q, r\} \qquad p$$

$Y = \{q, r\}$
$Pos([a]ff)$

$Inv(\ a\ tt)$

$$X \stackrel{\max}{=} \ a\ tt \quad [a]X.$$

$Pos([a]ff)$

$$Y \stackrel{\min}{=} [a]ff \quad \ a\ Y.$$

F

$Inv(F)$ F

$$X \stackrel{\max}{=} F \quad [\mathsf{Act}]X$$

F $Pos(F)$

$$Y \stackrel{\min}{=} F \quad \mathsf{Act}\ Y.$$

q *not* $Inv(\ a\ tt)$
a

$Pos(\ a\ tt)$
a
a

Exercise 7.2 , Pos
/ Inv, . .

7.1 Examples of recursive properties

$Safe(F)$ p

$$p = p_0 \stackrel{a_1}{\to} p_1 \stackrel{a_2}{\to} p_2 \cdots$$

p_i F *complete* *invariance of* F *under some computation*

$$X \stackrel{\max}{=} F \quad ([\mathsf{Act}]\mathit{ff} \quad \mathsf{Act}\ X).$$

p $Even(F)$ F p F p F

$$Y \stackrel{\min}{=} F \quad (\ \mathsf{Act}\ \mathit{tt} \quad [\mathsf{Act}]Y).$$

$Even(F)$ p

$Safe(F)$ $Even(F)$ $Inv(F)$ $Pos(F)$ *dual* $[A]$ A $\stackrel{\min}{=}$ $\stackrel{\max}{=}$ $\neg Inv(F) \equiv Pos(\neg F)$ $\neg Safe(F) \equiv Even(\neg F)$ $\neg$ F G

- $F\, \mathsf{U}^s\, G$ *strong until* p G F
- $F \mathsf{U}^w G$ *weak until* F p G !

$$F\, \mathsf{U}^s\, G \quad \stackrel{\min}{=} \quad G \quad (F \quad \mathsf{Act}\ \mathit{tt} \quad [\mathsf{Act}](F \mathsf{U}^s G)),$$
$$F\, \mathsf{U}^w\, G \quad \stackrel{\max}{=} \quad G \quad (F \quad [\mathsf{Act}](F \mathsf{U}^w G)).$$

strong until *weak until* $Even(F)$ $Inv(F)$ $Even(G) \equiv \mathit{tt}\, \mathsf{U}^s\, G$ $Inv(F) \equiv F\, \mathsf{U}^w\, \mathit{ff}$

temporal properties *Tempora*

temporal logic

μ

μ

not

7.2 Syntax and semantics of Hennessy-Milner logic with recursion

one

mutual recursion

X $\mathsf{M}_{\{X\}}$

$$F ::= X \mid tt \mid ff \mid F_1 \quad F_2 \mid F_1 \quad F_2 \mid \quad a \; F \mid [a]F.$$

F X

$\mathsf{O}_F : \mathsf{P}(\mathsf{Proc}) \rightarrow \mathsf{P}(\mathsf{Proc})$

X F

Example 7.2 $F = \; a \; X$ Proc

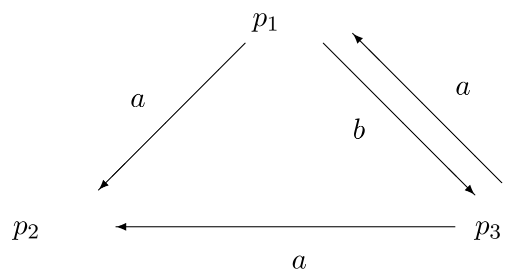
X p_1 $a \; X$

p_3

$$\mathsf{O}_{\; a \; X}(\{p_1\}) \; = \; \{p_3\}.$$

X $\{p_1, p_2\}$ $a \; X$ $\{p_1, p_3\}$

$$\mathsf{O}_{\; a \; X}(\{p_1, p_2\}) \; = \; \{p_1, p_3\}.$$



De inition 7.1 $(\mathsf{Proc}, \mathsf{Act}, \{\stackrel{a}{\to} \mid a \quad \mathsf{Act}\})$
S Proc F $O_F(S)$

$$\begin{array}{rcl} O_X(S) &=& S\\ O_{tt}(S) &=& \mathsf{Proc}\\ O_{ff}(S) &=& \\ O_{F_1 \ \ F_2}(S) &=& O_{F_1}(S) \cap O_{F_2}(S)\\ O_{F_1 \ \ F_2}(S) &=& O_{F_1}(S) \quad O_{F_2}(S)\\ O_{\ a\ F}(S) &=& \ \cdot a \cdot \ O_F(S)\\ O_{[a]F}(S) &=& [\cdot a \cdot] O_F(S) \end{array}$$

Exercise 7.3 .2, -
$O_{[b]ff \quad [a]X}(\{p_2\})$.

F O_F *monotonic*
$(P(\mathsf{Proc}), \quad)$ S_1, S_2 Proc
S_1 S_2 $O_F(S_1)$ $O_F(S_2)$

Exercise 7.4 O_F F.
.

O_F
$[\![X]\!]$ Proc X $O_F([\![X]\!])$
F $[\![X]\!]$
$[\![X]\!]$ X

$$X \stackrel{\min}{=} F_X \qquad X \stackrel{\max}{=} F_X.$$

$$[\![X]\!] = O_{F_X}([\![X]\!]).$$

O_{F_X}

O_{F_X}

maximal FIX O_{F_X}

minimal fix O_{F_X}

$$\text{FIX } O_{F_X} = \square \{S \quad \mathsf{Proc} \mid S \quad O_{F_X}(S)\}$$
$$\text{fix } O_{F_X} = \square \{S \quad \mathsf{Proc} \mid O_{F_X}(S) \quad S\}.$$

S S $O_{F_X}(S)$ *post fixed point* O_{F_X}

S *pre fixed point* O_{F_X} $O_{F_X}(S)$ S

$f : P(\mathsf{Proc}) \longrightarrow P(\mathsf{Proc})$

$f^0 = id_{P(\mathsf{Proc})}$ $P(\mathsf{Proc})$

$f^{m+1} = f \circ f^m.$

Proc

Theorem 7.1 Proc FIX $O_{F_X} = (O_{F_X})^M(\mathsf{Proc})$ M

fix $O_{F_X} = (O_{F_X})^m(\ )$ m

Proof:

□

7.3 Maximal fixed points and invariant properties

$$X \stackrel{\max}{=} F_X$$

$[\![X]\!]$ Proc

$$[\![X]\!] = \text{FIX } O_{F_X}.$$

invariant

$Inv(F)$

$$X = F \quad [\mathsf{Act}]X.$$

$Inv(F)$ *F holds under all transitions sequences*

$$I : 2^{\mathsf{Proc}} \longrightarrow 2^{\mathsf{Proc}}$$

$$I(S) = [\![F]\!] \cap [\cdot\mathsf{Act}\cdot]S.$$

$$\mathrm{FIX}\ I = \bigsqcup \{S \mid S \quad I(S)\}$$

$\mathrm{FIX}\ I$

F

Inv

$$Inv = \{p \mid \quad s \quad \mathsf{Act}\ , p \quad \mathsf{Proc}\ .\ p \xrightarrow{s} p \quad\quad p \quad [\![F]\!]\}.$$

$Inv(F)$

Theorem 7.2 $(\mathsf{Proc}, \mathsf{Act}, \{ \xrightarrow{a} \mid a \quad \mathsf{Act}\})$ $Inv\ =\ \mathrm{FIX}\ I$

Proof: $Inv \quad \mathrm{FIX}\ I$ $\mathrm{FIX}\ I \quad Inv$

$Inv \quad \mathrm{FIX}\ I$ $Inv \quad I(Inv)$ $p \quad Inv$ $s\ \ p$

$$p \xrightarrow{s} p \quad\quad p \quad [\![F]\!].$$

$p \quad I(Inv)$ $p \quad [\![F]\!]$ $p \quad [\cdot\mathsf{Act}\cdot]Inv$ $s = \varepsilon$ $p \xrightarrow{\varepsilon} p$ $p \quad [\cdot\mathsf{Act}\cdot]Inv$ p a

$p \xrightarrow{a} p$ p Inv

s

p

$p \xrightarrow{a} p$ $p \xrightarrow{s'} p$ p $[\![F]\!]$

$s = as$

FIX I Inv FIX I I

$$\text{FIX } I = [\![F]\!] \cap [\cdot\text{Act}\cdot]\text{FIX } I.$$

FIX I Inv p FIX I $p \xrightarrow{s} p$

p $[\![F]\!]$ $|s|$ s

$s = \varepsilon$ $p = p$ p $[\![F]\!]$

$s = as$ $p \xrightarrow{a} p \xrightarrow{s'} p$ p

p FIX I $|s| < |s|$ p FIX I

p $[\![F]\!]$

$\square$

7.4 Game Characterization of Hennessy-Milner Logic with One Recursively Defined Variable

To be connected with the rest of the text.

X

$$F ::= X \mid tt \mid ff \mid F_1 \quad F_2 \mid F_1 \quad F_2 \mid \quad a \ F \mid [a]F$$

a Act X

$$X \overset{\min}{=} F_X$$

$$X \overset{\max}{=} F_X$$

F_X

X

$(\mathsf{Proc}, \mathsf{Act}, \{\xrightarrow{a} \mid a \quad \mathsf{Act}\})$ F
X s Proc

- $s \models F$
- $s \models F$

configurations (s, F) s Proc F
X

F s Proc

- (s, tt) (s, ff)
- $(s, F_1 \quad F_2)$ $(s, F_1 \quad F_2)$
  (s, F_1) (s, F_2)
- $(s, \ a \ F)$ $(s, [a]F)$ $(s \ , F)$
  s $s \xrightarrow{a} s$
- (s, X) (s, F_X) X
  $X \overset{\max}{=} F_X$ $X \overset{\min}{=} F_X$

play (s, F)

- $(s, F_1 \quad F_2)$ $(s, [a]F)$
- $(s, F_1 \quad F_2)$ $(s, \ a \ F)$

(s, X)
$(s, X) \ \to \ (s, F_X)$
$\xrightarrow{A}$

$\xrightarrow{D}$

- (s, tt) (s, ff)
- $(s, [a]F)$ $(s, \ a \ F)$ $s \stackrel{a}{\not\to}$

-

-
  (s, ff)

-
  (s, tt)

- X
  $X \stackrel{\min}{=} F_X$ X
  $X \stackrel{\max}{=} F_X$

Theorem 7.3
$(\mathsf{Proc}, \mathsf{Act}, \{\stackrel{a}{\to} \mid a \quad \mathsf{Act}\})$ F
X s Proc

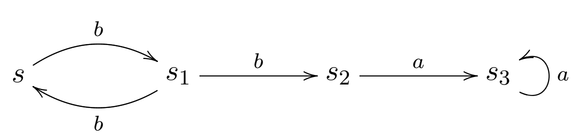
- $s \models F$
  (s, F)

- $s \models F$
  (s, F)

Remark 7.1 X

X

7.4.1 Examples of Use



Example 7.3
$s \models [b](\ b\ [b]\mathit{ff} \quad b\ [a]\mathit{ff})$
$\stackrel{A}{\to}$
$\stackrel{D}{\to}$
$(s, [b](\ b\ [b]\mathit{ff}$

$b\ [a]\mathit{ff}))$ $[b]$

$$(s,[b](\ b\ [b]\mathit{ff}\quad b\ [a]\mathit{ff})) \xrightarrow{A} (s_1,\ b\ [b]\mathit{ff}\quad b\ [a]\mathit{ff}).$$

$$(s_1,\ b\ [b]\mathit{ff}\quad b\ [a]\mathit{ff}) \xrightarrow{A} (s_1,\ b\ [b]\mathit{ff})$$

$$(s_1,\ b\ [b]\mathit{ff}\quad b\ [a]\mathit{ff}) \xrightarrow{A} (s_1,\ b\ [a]\mathit{ff}).$$

- $(s_1,\ b\ [b]\mathit{ff})$
  $(s_1,\ b\ [b]\mathit{ff}) \xrightarrow{D} (s_2,[b]\mathit{ff})$ $s_2 \stackrel{b}{\nrightarrow}$

- $(s_1,\ b\ [a]\mathit{ff})$
  $(s_1,\ b\ [a]\mathit{ff}) \xrightarrow{D} (s,[a]\mathit{ff})$ $s \stackrel{a}{\nrightarrow}$

Example 7.4 $X \stackrel{\min}{=} a\ \mathit{tt}\quad b\ X$
b a
$s \models X$
(s,X)
$\xrightarrow{D}$ $\rightarrow$ X

$$(s,X) \rightarrow (s,\ a\ \mathit{tt}\quad b\ X) \xrightarrow{D} (s,\ b\ X) \xrightarrow{D} (s_1,X) \rightarrow$$

$$\rightarrow (s_1,\ a\ \mathit{tt}\quad b\ X) \xrightarrow{D} (s_1,\ b\ X) \xrightarrow{D} (s_2,X) \rightarrow$$

$$\rightarrow (s_2,\ a\ \mathit{tt}\quad b\ X) \xrightarrow{D} (s_2,\ a\ \mathit{tt}) \xrightarrow{D} (s_3,\mathit{tt})$$

(s_3,tt)

Example 7.5 $X \stackrel{\max}{=} b\ tt \quad [b]X$

b b

$s \models X$

(s, X)

$$(s, X) \rightarrow (s,\ b\ tt \quad [b]X) \xrightarrow{A} (s, [b]X) \xrightarrow{A} (s_1, X) \rightarrow$$

$$\rightarrow (s_1,\ b\ tt \quad [b]X) \xrightarrow{A} (s_1, [b]X) \xrightarrow{A} (s_2, X) \rightarrow$$

$$\rightarrow (s_2,\ b\ tt \quad [b]X) \xrightarrow{A} (s_2,\ b\ tt)$$

$(s_2,\ b\ tt)$

$s_2 \stackrel{b}{\not\rightarrow}$

Example 7.6 $X \stackrel{\max}{=} a\ tt \quad [a]X$

a b $s_2 \models X$

(s_2, X)

X $(s_2, X) \rightarrow (s_2,\ a\ tt \quad [a]X)$

$$(s_2,\ a\ tt \quad [a]X) \xrightarrow{A} (s_2,\ a\ tt)$$

$$(s_2,\ a\ tt \quad [a]X) \xrightarrow{A} (s_2, [a]X).$$

$(s_2,\ a\ tt)$

$(s_2,\ a\ tt) \xrightarrow{D} (s_3, tt)$

$(s_2, [a]X)$ $(s_2, [a]X) \xrightarrow{A} (s_3, X)$

X $(s_3,\ a\ tt \quad [a]X)$

$$(s_3,\ a\ tt \quad [a]X) \xrightarrow{A} (s_3,\ a\ tt)$$

$$(s_3,\ a\ tt \quad [a]X) \xrightarrow{A} (s_3, [a]X).$$

$$(s_3, [a]X) \xrightarrow{A} (s_3, X)$$

Example 7.7 $X \stackrel{\min}{=} a\ tt \quad ([b]X \quad b\ tt)$
b a
$s_1 \models X$
(s_1, X) $(s_1, X) \to (s_1, a\ tt \quad ([b]X$
$b\ tt))$

$$(s_1, a\ tt \quad ([b]X \quad b\ tt)) \xrightarrow{D} (s_1, a\ tt)$$

$$(s_1, a\ tt \quad ([b]X \quad b\ tt)) \xrightarrow{D} (s_1, [b]X \quad b\ tt).$$

a
s_1 $s_1 \stackrel{a}{\not\to}$

$$(s_1, [b]X \quad b\ tt) \xrightarrow{A} (s_1, [b]X) \xrightarrow{A} (s, X)$$

(s, X) $(s, X) \to (s, a\ tt \quad ([b]X$
$b\ tt))$ $(s, a\ tt \quad ([b]X \quad b\ tt)) \xrightarrow{D} (s, a\ tt)$
$(s, a\ tt \quad ([b]X \quad b\ tt)) \xrightarrow{D}$
$(s, [b]X \quad b\ tt)$ $(s, [b]X \quad b\ tt) \xrightarrow{A} (s, [b]X) \xrightarrow{A} (s_1, X)$
(s_1, X)

7.5 Mutually recursive equational system

mutually recursive equational system

$$X_1 = F_{X_1}$$

$$X_n = F_{X_n} ,$$

$\mathsf{X} = \{X_1, \ldots, X_n\}$ $i \leq n$ F_{X_i}
M_X X

$$X = [a]Y$$
$$Y = a\ X\ .$$

X declaration $D : X \to M_X$

$D(X) = F_X$

n dimensional vectors

n X $D = (P(\mathrm{Proc}))^n$

n $P(\mathrm{Proc})$

$$(S_1, \ldots, S_n) \leq (S_1, \ldots, S_n) \quad S_1 \quad S_1 \quad S_2 \quad S_2 \quad \ldots \quad S_n \quad S_n.$$

$(D, \leq)$

$$\bigsqcup\{(A_1^i, \ldots, A_n^i) \mid i \quad I\} = (\bigsqcup\{A_1^i \mid i \quad I\}, \ldots, \bigsqcup\{A_n^i \mid i \quad I\})$$

$$\bigsqcap\{(A_1^i, \ldots, A_n^i) \mid i \quad I\} = (\bigsqcup\{A_1^i \mid i \quad I\}, \ldots, \bigsqcup\{A_n^i \mid i \quad I\}).$$

$$[\![D]\!] : D \to D$$

D

$$[\![D]\!]([\![X_1]\!], \ldots, [\![X_n]\!]) = (O_{F_{X_1}}([\![X_1]\!], \ldots, [\![X_n]\!]), \ldots, O_{F_{X_n}}([\![X_1]\!], \ldots, [\![X_n]\!])) ,$$

$[\![X_i]\!]$ $1 \leq i \leq n$ S Proc

$[\![D]\!]$ $(D, \leq)$

Exercise 7.5

1. $(P(\mathrm{Proc})^n, \leq, \bigsqcup, \bigsqcap)$, $\leq$, $\bigsqcup$ $\bigsqcap$

 , .

2. (30)

$$[\![D]\!] : P(\mathrm{Proc})^n \longrightarrow P(\mathrm{Proc})^n .$$

3.

$$X = [a]Y$$
$$Y = a \; X$$

$$
\begin{aligned}
A_0 &= a.A_1 + a.a.0 \\
A_1 &= a.A_2 + a.0 \\
A_2 &= a.A_1 \quad .
\end{aligned}
$$

7.6 A Proof System for Maximal Properties

p F

sound *complete*

X

$$X \stackrel{\max}{=} F_X \quad .$$

axiom

Γ $p : F$ Γ

hypotheses

$$\{p_1 : X, \ldots, p_n : X\} \quad .$$

sequents

Γ $p : F$

$\Gamma = \{p_1 : X, \ldots, p_n : X\}$

p_i $[\![X]\!]$ i p F

p $[\![F]\!]$

TT $$\Gamma \quad p : tt$$

AND $$\frac{\Gamma \quad p : F_1 \quad \Gamma \quad p : F_2}{\Gamma \quad p : F_1 \quad F_2}$$

OR $$\frac{\Gamma \quad p : F_1}{\Gamma \quad p : F_1 \quad F_2} \qquad \frac{\Gamma \quad p : F_2}{\Gamma \quad p : F_1 \quad F_2}$$

DIAMOND $$\frac{\Gamma \quad p' : F}{\Gamma \quad p : \; a \; F} \qquad p \xrightarrow{a} p'$$

BOX $$\frac{\Gamma \quad p_1 : F \; \cdots \; \Gamma \quad p_n : F}{\Gamma \quad p : [a]F} \qquad \{p_1, \ldots, p_n\} = \{p \mid p \xrightarrow{a} p'\}$$

MAX1 $$\Gamma, p : X \quad p : X$$

MAX2 $$\frac{\Gamma, p : X \quad p : F_X}{\Gamma \quad p : X} \qquad X \overset{\mathsf{max}}{=} F_X$$

$$
\dfrac{\dfrac{\dfrac{p : X}{p : X \quad p : \ a \ tt \quad [a]X}\text{MAX2}}{\dfrac{p : X \quad p : [a]X}{p : X \quad p : X}\text{BOX} \quad \dfrac{p : X \quad p : \ a \ tt}{p : X \quad p : tt}\text{DIAMOND}}\text{AND}}{}
$$

$p \models Inv(\ a \ tt)$

TT

p tt

MAX1 p X

$\Gamma \quad p : F$

TT MAX1

$\Gamma \quad p : F \quad \Gamma \quad p : F \quad \Gamma \quad p : F$

Example 7.8 p

$p \models Inv(\ a \ tt)$

MAX1

TT

soundness

complete

$$p : F \quad p \quad [\![F]\!].$$

Lemma 7.1 $(\mathsf{Proc}, \mathsf{Act}, \{ \xrightarrow{a} | a \quad \mathsf{Act}\})$

p F

$p \quad [\![F]\!] \quad S \quad \mathsf{Proc} \quad S \quad O_{F_X}(S) \quad p \quad O_F(S).$

Exercise 7.6 *.1* . *(*

F.)

$p : F$ S Proc S $\mathsf{O}_{F_X}(S)$ p $\mathsf{O}_F(S)$.

Theorem 7.4 X $X \stackrel{\max}{=} F_X$ E

$p_1 : X, \ldots, p_n : X$ $p : F$ S $\mathsf{O}_{F_X}(S)$ $\{p_1, \ldots, p_n\}$ S p $\mathsf{O}_F(S)$

Proof: $p_1 : X, \ldots, p_n : X$ $p : F$

Base case: TT `Max1`

TT $F = tt$ $\mathsf{O}_F(S) =$ Proc S S Proc S $\mathsf{O}_{F_X}(S)$ $\{p_1, \ldots, p_n\}$ p $\mathsf{O}_F(S)$ $S =$

MAX1 $p_1 : X, \ldots, p_n : X, p : X$ $p : X$ S $S = \{p\}$

Inductive step:

MAX2 $p_1 : X, \ldots, p_n : X$ $p : X$

$p_1 : X, \ldots, p_n : X, p : X$ $p : F_X$.

S $\mathsf{O}_{F_X}(S)$ $\{p_1, \ldots, p_n, p\}$ p $\mathsf{O}_{F_X}(S)$ S S S $\mathsf{O}_{F_X}(S\ )$ $\{p_1, \ldots, p_n\}$ p $\mathsf{O}_X(S\ )$ $S\ = S$ $\{p\}$

□

Exercise 7.7 . .
$S = S \quad \{p\}$ MAX2

Exercise 7.8 . *(31)*.

sound

complete

Theorem 7.5 p *finite*
S Proc S $\mathsf{O}_{F_X}(S)$ $\{p_1, \ldots, p_n\}$ p $\mathsf{O}_F(S)$
$p_1 : X, \ldots, p_n : X$ $p : F$

Proof: $(\mathsf{Proc}, \mathsf{Act}, \{a \quad \mathsf{Act} \mid \overset{a}{\to} \})$
$\mathsf{Proc} = \{q_1, \ldots, q_k\}$ k S
S $\mathsf{O}_{F_X}(S)$ $\{p_1, \ldots, p_n\}$ p $\mathsf{O}_F(S)$

$p_1 : X, \ldots, p_n \quad p : F$

$|\mathsf{Proc} \setminus \{p_1, \ldots p_n\}|$
$\{p_1, \ldots, p_n\}$

Base case: $\{p_1, \ldots, p_n\} = \mathsf{Proc}$
F

$F = tt$**:** TT

$F = F_1 \quad F_2$**:** S $\mathsf{O}_{F_X}(S)$ $\{p_1, \ldots, p_n\}$ p
$\mathsf{O}_{F_1 \ F_2}(S)$ $\mathsf{O}_{F_1 \ F_2}$ p $\mathsf{O}_{F_1}(S)$ p
$\mathsf{O}_{F_1}(S)$
$p_1 : X, \ldots p_k : X \quad F_1 \quad p_1 : X, \ldots p_k : X \quad F_2$
AND $p_1 : X, \ldots, p_n \quad p : F_1 \quad F_2$

$F = X$**:** $p \quad \{p_1, \ldots, p_n\}$
MAX1

Inductive step: P Proc $|P| <$
$n - k$ S
S $\mathsf{O}_{F_X}(S)$ $\{p_1, \ldots, p_n\}$ p $\mathsf{O}_F(S)$
$p_1 : X, \ldots, p_n \quad p : F$ F

$F = X \quad p \quad \{p_1, \ldots, p_n\}$

MAX1 $\quad p \quad \{p_1, \ldots, p_n\}$

$R.(R \quad \mathsf{O}_{F_X}(R) \quad p \quad \mathsf{O}_{F_X}(R) \quad \{p_1, \ldots, p_n, p\})$

$p_1 : X, \ldots, p_n : X, p : X \quad p : F_X$

$S \quad S \quad \mathsf{O}_{F_X}(S) \quad \{p_1, \ldots, p_n\}$

$p \quad \mathsf{O}_X(S)$

$$S \quad \mathsf{O}_{F_X}(S) \quad \{p_1, \ldots, p_n, p\}.$$

$\mathsf{O}_X(S) = S$

$$p \quad \mathsf{O}_X(S) = S \quad \mathsf{O}_{F_X}(S) \quad \{p_1, \ldots, p_n\}.$$

$p \quad \{p_1, \ldots, p_n\}$

$$p \quad \mathsf{O}_{F_X}(S).$$

$$p_1 : X, \ldots, p_n : X, p : X \quad p : F_X.$$

MAX2

$$p_1 : X, \ldots, p_n : X \quad p : X \quad ,$$

$\square$

7.7 Characteristic properties

p

$p \quad [p] \quad = \{q \mid q \quad p\}$

$$[p] \quad = \{q \mid \quad F \quad \mathsf{M}.p \models F \ = \quad q \models F\}.$$

Exercise 7.9

, p q,

. , , q

p, p q *same* .

single

p *characteristic formula for* p

$[p]$

p

ϕ_p M_X X

q

$q \models \phi_p$ q p.

Example 7.9 Act $= \{a\}$ p

$$X = a.X.$$

p

ϕ M

$$[\![\phi]\!] = [p] \; .$$

$$p \models \phi \qquad q.\, q \models \phi \; = \quad q \quad p.$$

ϕ

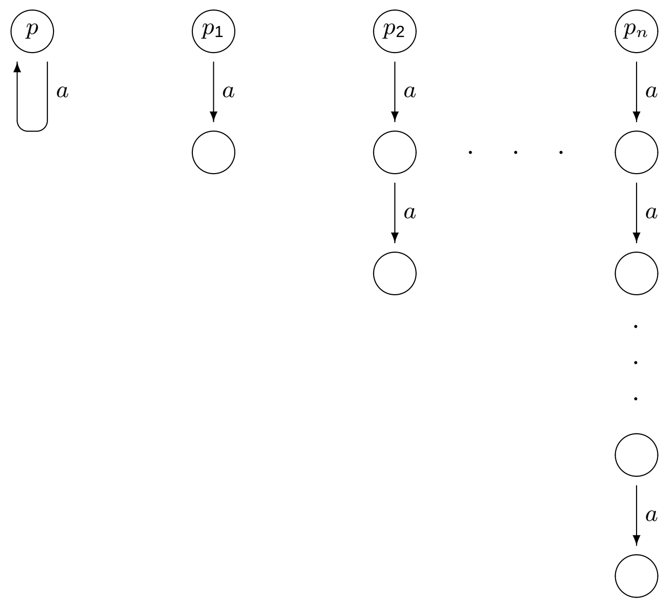
modal depth ϕ $md(\phi)$

ϕ

$$md(tt) = md(ff) = 0$$

$$md([a]\phi) = md(\; a \; \phi) = 1 + md(\phi)$$

$$md(\phi_1 \quad \phi_2) = md(\phi_1 \quad \phi_2) = \max\{md(\phi_1), md(\phi_2)\}$$



p p_i $i \leq n$

$p_0, p_1, p_2, \ldots$

$p_0 = \mathbf{0}$

$p_{i+1} = a.p_i$

p p_i $i \geq 1$

ϕ. $p \models \phi$ $p_{md(\phi)} \models \phi$.

ϕ

p p_n n

ϕ p

$$(\{p_1, \ldots, p_n\}, \mathsf{Act}, \rightarrow)$$

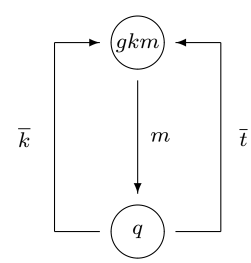
$$\mathsf{X} = \{X_{p_1}, \ldots, X_{p_n}, \ldots\}$$

X_p

p

can perform *cannot perform* *after it has performed*

Example 7.10



gkm

gkm gkm

m

gkm m

q

gkm m q

gkm m q

gkm m

X_{gkm} X_q q gkm

X_{gkm}

$$X_{gkm} \equiv \quad m \; X_q \quad [m]X_q \quad [\overline{t}, \overline{k}]ff$$

$m\ X_q$ $[m]X_q$ $[\bar{t},\bar{k}]ff$

gkm X_q

q $\bar{t}$ $\bar{k}$

$gkm\ X_q$

$$X_q \equiv \bar{t}\ X_{gkm} \quad \bar{k}\ X_{gkm} \quad [\bar{t},\bar{k}]X_{gkm} \quad [m]ff$$

$$Der(a,p) = \{p \mid p \xrightarrow{a} p\}.$$

p $Der(a,p)$ p $X_{p'}$ p
$a\ X_{p'}$ a

$$p \models \bigvee_{a,p'.p \xrightarrow{a} p'} a\ X_{p'}$$

$p \xrightarrow{a} p$ p $Der(a,p)$ p

$$[a] \bigvee_{p'.p \xrightarrow{a} p'} X_{p'} ,$$

a

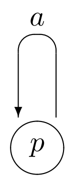
$$p \models \bigwedge_{a} [a] \bigvee_{p'.p \xrightarrow{a} p'} X_{p'}$$

$$p \models \bigvee_{a,p'.p \xrightarrow{a} p'} a\ X_{p'} \quad \bigwedge_{a} [a] \bigvee_{p'.p \xrightarrow{a} p'} X_{p'}$$

p
$p\ X_p$

q Proc

$$X_q \equiv \bigvee_{a,q'.q \xrightarrow{a} q'} a\ X_{q'} \quad \bigwedge_{a} [a] \bigvee_{q'.q \xrightarrow{a} q'} X_{q'}$$



p

Example 7.11 p

$$X_p \overset{\min}{=} a\ X_p \quad [a]X_p$$

$X_p = ff$ p
ff p

p Proc

Theorem 7.6 (Proc, Act, $\rightarrow$) p
Proc X_p

$$X_p \overset{\max}{=} \underset{a,p'.p \overset{a}{\to} p'}{\square} a\ X_{p'} \quad \underset{a}{\square}[a]\underset{p'.p \overset{a}{\to} p'}{\square} X_{p'}.$$

X_p p

Proc Act

D_K

$$D_K(X_p) = \underset{a,p.p \overset{a}{\to} p'}{\square} a\ X_{p'} \quad \underset{a}{\square}[a]\underset{p'.p \overset{a}{\to} p'}{\square} X_{p'}.$$

X_p
p $[\![X_p]\!]$ p Proc
$[\![X_p]\!] = [p]$ $q \models_{max} X_p$ q $[\![X_p]\!]$
D_K

Lemma 7.2 X_p

$$q \models_{max} X_p \quad p \quad q$$

Proof: $R = \{(p,q) \mid q \models_{max} X_p\}$ R
p q

$$(p,q) \quad R \quad p \xrightarrow{b} p_1 \quad q_1 .\, q \xrightarrow{b} q_1 \quad (p_1, q_1) \quad R.$$
$$(p,q) \quad R \quad q \xrightarrow{b} q_1 \quad p_1 .\, p \xrightarrow{b} p_1 \quad (p_1, q_1) \quad R.$$

a) (p,q) R $p \xrightarrow{b} p_1$

$$q \models_{max} X_p \quad p \xrightarrow{b} p_1$$

$$X_p \quad D_K$$

$$q \models_{max} X_p \overset{\max}{=} q \models_{max} \Big(\underset{a, p'.p \xrightarrow{a} p'}{\Box} a \; X_{p'} \Big) \quad \Big(\underset{a}{\Box} [a] \underset{p'.p \xrightarrow{a} p'}{\Box} X_{p'} \Big)$$

$p \xrightarrow{b} p_1$ $q \models_{max} b \; X_{p_1}$

$$q_1 .\, q \xrightarrow{b} q_1 \quad q_1 \models_{max} X_{p_1}$$

$$q_1 . q \xrightarrow{b} q_1 \quad (p_1, q_1) \quad R.$$

b) (p,q) R $q \xrightarrow{b} q_1$

$$q \models_{max} X_p \quad q \xrightarrow{b} q_1$$

$$q \models_{max} X_p \;=\; q \models_{max} \Big(\underset{a, p.p \xrightarrow{a} p'}{\Box} a \; X_{p'} \Big) \quad \Big(\underset{a}{\Box} [a] \underset{p'.p \xrightarrow{a} p'}{\Box} X_{p'} \Big) \; .$$

$$q \models_{max} [b] \underset{p'.p \xrightarrow{b} p'}{\Box} X_{p'}$$

$$q \xrightarrow{b} q \quad q \models_{max} \bigvee_{p'.p \xrightarrow{b} p'} X_{p'} \, .$$

$q \xrightarrow{b} q_1$

$$q_1 \models_{max} \bigvee_{p'.p \xrightarrow{b} p'} X_{p'} \, .$$

$$p_1 \qquad q_1 \models_{max} X_{p_1} \qquad p \xrightarrow{b} p_1$$

$$p_1 . \, p \xrightarrow{b} p_1 \qquad (p_1, q_1) \quad R \, .$$

R

$$q \models_{max} X_p \; = \quad p \quad q$$

$\square$

Lemma 7.3 $([p_1] \;, \ldots, [p_n] \;) \quad [\![D_K]\!]([p_1] \;, \ldots, [p_n] \;)$

Proof: $q \quad [p] \qquad p \qquad p_1, \ldots, p_n$

$$q \quad (\bigvee_{a,p'.p \xrightarrow{a} p'} \cdot a \cdot \; [p\,] \;) \;\cap\; (\bigwedge_{a} [\cdot a \cdot] \bigvee_{p'.p \xrightarrow{a} p'} [p\,] \;).$$

$$q \quad \bigvee_{a,p'.p \xrightarrow{a} p'} \cdot a \cdot \; [p\,]$$

$$q \quad \bigwedge_{a} [\cdot a \cdot] \bigvee_{p'.p \xrightarrow{a} p'} [p\,]$$

1) $q \quad p \qquad p \xrightarrow{a} p \qquad q \qquad q \xrightarrow{a} q$
$q \quad p$

$$a, p \,, p \xrightarrow{a} p \, . \, (\; q \, . \, q \xrightarrow{a} q \qquad q \quad [p\,] \;)$$

$$q \quad \bigvee_{a,p'.p \xrightarrow{a} p'} \cdot a \cdot \; [p\,]$$

2) a Act $q \xrightarrow{a} q$ q $\square_{p'.p \xrightarrow{a} p'} [p\,]$ p q

p $p \xrightarrow{a} p$ q p

q $[p\,]$

$$a, q\,.\,q \xrightarrow{a} q \quad p\,.\,p \xrightarrow{a} p \quad q \quad [p\,] \ ,$$

$$q \quad \square_{a} [\cdot a \cdot] \quad \square_{p'.p \xrightarrow{a} p'} [p\,] \ .$$

$$([p_1] \ , \ldots, [p_n] \ ) \quad [\![D_K]\!]([p_1] \ , \ldots, [p_n] \ )$$

$\square$

Lemma 7.4 p Proc $[\![X_p]\!] = [p]$

Proof:

$$([p_1] \ , \ldots, [p_n] \ ) \leq ([\![X_{P_1}]\!], \ldots, [\![X_{P_n}]\!])$$

$[p]$ $[\![X_p]\!]$ p Proc

$[\![X_p]\!]$ $[p]$ p Proc $\square$

7.8 Mixing maximal and minimal fixed points

mixed solutions

$$X \overset{\max}{=} a\ Y$$
$$Y \overset{\min}{=} b\ X.$$

modal μ-calculus

nested mutual recursion

De inition 7.2 n E n

$$(D_1, X_1, m_1), (D_2, X_2, m_2), \ldots, (D_n, X_n, m_n) \ ,$$

$i \leq n$

- X_i
- $D_i : X_i \longrightarrow \prod_{j \leq i} X_i$
- $m_i = \max$ $m_i = \min$

A.1 Complete Lattices

De inition A.1 *partially ordered set (poset)*
$(D, \ )$ D D $D \times D$

-

De inition A.2 $(D, \quad)$
X D

- d D *upper bound* X x d□ x X
  d *least upper bound (lub)* X □ X d
  X d d d D
  X

- d D *lower bound* X d x x X
  d *greatest lower bound (glb)* X $\prod X$ d
  X d d d D
  X

Exercise A.2 $(D, \quad)$, X D.
X , .

Example A.2

- $(\quad , \leq)$

- □ $(P(S), \quad)$ *every* X $P(S)$ □ X
  X

Exercise A.3

1. □ X $P(S)$ □ X
   X, .

2. A $(A \;, \leq)$.

De inition A.3 $(D, \quad)$ *complete lattice* □ X
$\prod X$ X D

$(D, \quad)$ $= \prod D$
$\top =$ □ D

Exercise A.4 $(D, \quad)$. □ $\prod$

Example A.3

- $(\ ,\leq)$ *not*
- $(\quad \{\infty\},\ )$ ∞ $(\ ,\leq)$

$$\begin{array}{c}\infty\\ \\ \uparrow\\ 2\\ \uparrow\\ 1\\ \uparrow\\ 0\end{array}$$

- $(P(S),\ )$

A.2 Tarski's Fixed Point Theorem

Definition A.4 $(D,\ )$ $f : D \to D$ *monotonic* d, d D d d $f(d)$ $f(d\ )$ d D *fixed point* f $d = f(d)$

Theorem A.1 $(D,\ )$ $f : D \to D$ f $z_{\max}$ $z_{\min}$

$$z_{\max} = \bigsqcup\{x \quad D \mid x \quad f(x)\}$$
$$z_{\min} = \bigsqcap\{x \quad D \mid f(x) \quad x\}$$

Proof: $z_{\max}$ f

$z_{\max}$ f $z_{\max} = f(z_{\max})$

d D f d $z_{\max}$

$$A = \{x \quad D \mid x \quad f(x)\}.$$

$z_{\max}$ f

$$z_{\max} \quad f(z_{\max})$$
$$f(z_{\max}) \quad z_{\max}.$$

$$z_{\max} = \square\, A.$$

x A x $z_{\max}$ f x $z_{\max}$
$f(x)$ $f(z_{\max})$ x A x $f(x)$
$f(z_{\max})$ $f(z_{\max})$ A $z_{\max}$
least upper bound A $z_{\max}$ $f(z_{\max})$

f
$f(z_{\max})$ $f(f(z_{\max}))$ $f(z_{\max})$ A
$f(z_{\max})$ $z_{\max}$ $z_{\max}$ A

$z_{\max}$ $f(z_{\max})$ $z_{\max}$
$z_{\max} = f(z_{\max})$ $z_{\max}$ f

$z_{\max}$ f d
f d $f(d)$
d A d $\square\, A = z_{\max}$

$z_{\max}$ f

$z_{\min}$ f

$z_{\min}$ f $z_{\min} = f(z_{\min})$

d D f $z_{\min}$ d

$z_{\min}$ f

$$f(z_{\min}) \quad z_{\min}$$
$$z_{\min} \quad f(z_{\min}).$$

$z_{\min}$ f
f $\square$

Exercise A.5 (23) (2) .

1.

2. (23)
.3

3. -
(2).

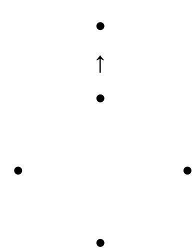
Exercise A.6

1. $(D, \;)$ $f : D \to D$ (1 , 103),

$$(\{x \;\; D \mid f(x) = x\}, \;)$$

f .

2. $(D, \;)$
$f : D \to D$ x, y D f,
$\{x, y\}$ *not* . *Hint* D



$f : D \to D$.

3. $(D, \;)$, $f : D \to D$. -
X $\{x \;\; D \mid x \;\; f(x)\}$.

( ) X $\{x \;\; D \mid x \;\; f(x)\}$.

( ) , , $\bigsqcap X$ $\{x \;\; D \mid x$
$f(x)\}$. *Hint* ,
.

. $(D, \;)$, $f : D \to D$. -
X $\{x \;\; D \mid f(x) \;\; x\}$.

( ) $\prod X$ $\{x$ $D \mid f(x)$ $x\}$.

( ) , , $\square X$ $\{x$ $D \mid f(x)$ $x\}$. *Hint* 2 .

. $(D,$ $)$.

( ) $D \rightarrow_{mon} D$ D D $D \rightarrow_{mon} D$

$$f \quad g \quad d \quad D.\, f(d) \quad g(d).$$

$D \rightarrow_{mon} D$.

( ) $\square$ $\square$ $D \rightarrow_{mon} D$

F $D \rightarrow_{mon}$

D D

m $f^k(\ ) = f^m(\ )$ $k \geq m$ $f(f^m(\ )) =$
$f^{m+1}(\ ) = f^m(\ )$ $f^m(\ )$ f
$f^m(\ )$ f d
f d f
$f(\ )$ $f(d) = d$ $m-1$
$f^m(\ )$ d $f^m(\ )$ f

□

A.3 Bisimulation as a Fixed Point

$(\mathsf{Proc}, \mathsf{Act}, \{ \xrightarrow{a} \mid a \quad \mathsf{Act}\})$
S $\mathsf{Proc} \times \mathsf{Proc}$ *strong bisimulation*

(p, q) S α Act

$p \xrightarrow{\alpha} p$ $q \xrightarrow{\alpha} q$ q (p, q) S

$q \xrightarrow{\alpha} q$ $p \xrightarrow{\alpha} p$ p (p, q) S

strong bisimulation equivalence *strong equality*

$$= \quad \{S \quad \mathcal{P}(\mathsf{Proc} \times \mathsf{Proc}) \mid S \quad \}.$$

$(\mathcal{P}(\mathsf{Proc} \times \mathsf{Proc}), \ )$
Proc
! $\mathcal{F} : \mathcal{P}(\mathsf{Proc} \times \mathsf{Proc}) \longrightarrow$
$\mathcal{P}(\mathsf{Proc} \times \mathsf{Proc})$

(p, q) $\mathcal{F}(S)$

$p \xrightarrow{\alpha} p$ $q \xrightarrow{\alpha} q$ q (p, q) S

$q \xrightarrow{\alpha} q$ $p \xrightarrow{\alpha} p$ p (p, q) S

S S $\mathcal{F}(S)$

$$= \quad \{S \quad \mathcal{P}(\mathsf{Proc} \times \mathsf{Proc}) \mid S \quad \mathcal{F}(S)\}.$$

S, R $\mathcal{P}(\mathsf{Proc} \times \mathsf{Proc})$ S R $\mathcal{F}(S)$ $\mathcal{F}(R)$
! $\mathcal{F}$ $(\mathcal{P}(\mathsf{Proc} \times \mathsf{Proc}), \ )$

F Proc
$F^M(\mathsf{Proc} \times \mathsf{Proc})$ $M \geq 0$

$F^i(\mathsf{Proc}\times\mathsf{Proc})$ $i \geq 0$

Example A.4

$$
\begin{aligned}
Q_1 &= b.Q_2 + a.Q_3 \\
Q_2 &= c.Q_4 \\
Q_3 &= c.Q_4 \\
Q_4 &= b.Q_2 + a.Q_3 + a.Q_1 \ .
\end{aligned}
$$

$$\mathsf{Proc} = \{Q_i \mid 1 \leq i \leq 4\} \ .$$

I Proc

$$I = \{(Q_i, Q_i) \mid 1 \leq i \leq 4\} \ .$$

$F^i(\mathsf{Proc} \times \mathsf{Proc})$ $i \geq 1$

$$
\begin{aligned}
F^1(\mathsf{Proc} \times \mathsf{Proc}) &= \{(Q_1, Q_4), (Q_4, Q_1), (Q_2, Q_3), (Q_3, Q_2)\} \quad I \\
F^2(\mathsf{Proc} \times \mathsf{Proc}) &= \{(Q_2, Q_3), (Q_3, Q_2)\} \quad I \\
F^3(\mathsf{Proc} \times \mathsf{Proc}) &= F^2(\mathsf{Proc} \times \mathsf{Proc}) \ .
\end{aligned}
$$

Q_2 Q_3

Exercise A.7

1. ,

$$
\begin{aligned}
P_1 &= a.P_2 \\
P_2 &= a.P_1 \\
P_3 &= a.P_2 + a.P_4 \\
P_4 &= a.P_3 + a.P_5 \\
P_5 &= 0 \ .
\end{aligned}
$$

2.

n m

3.

.

Acknowledgments

References

A brief history of process algebra

On the consistency of Koomen's fair abstraction rule

Process Algebra

Graphical versus logical specifications

Automatic verification of finite-state concurrent systems using temporal logic specifications

Generative communication in Linda.

The linear time–branching time spectrum. I. The semantics of concrete, sequential processes

On the development of reactive systems

Algebraic laws for nondeterminism and concurrency

Communicating sequential processes

—— *Communicating Sequential Processes*

Formal verification of parallel programs

Results on the propositional mu-calculus

Proof systems for satisfiability in Hennessy–Milner logic with recursion

Communication and Concurrency

Semantics with Applications: A Formal Introduction &

Concurrency and automata on infinite sequences 5^{th}

A structural approach to operational semantics

—— *The origins of structural operational semantics*

—— *A structural approach to operational semantics.*

The temporal logic of programs *18*th

Local model checking games

A lattice-theoretical fixpoint theorem and its applications

On the Ehrenfeucht-Fraïssé game in theoretical computer science (extended abstract)