Concurrency and Process Logics

Ken Stevens
Verification

Cannot understand verification
without understanding concurrency
Concurrency Challenge

Concurrency is major challenge

- practically: plethora of concurrent implementations
  - architectures
    - Mayfly, transputer, reduction machines, microprocessors, . . .
  - Programming
    - Algorithms, actors, domains, threads, . . .

- Theoretical: model and prove properties
  - architectures
    - PRAM model, . . .
  - Programming
    - CSP, Occam, CCS, . . .
Concurrency

Interesting dichotomy exists:

- more parallel architectures than languages
  - inherent parallelism in hardware
  - inherent difficulty in parallel programming
    - perhaps Verilog is most used parallel programming language?

Humans don’t think in parallel

- missed off-ramp on freeway
Concurrency Models

Plethora of variations can create confusion

Theory is useful

- provides clarity and understanding
- classifies/groups similarities/variations
- applicable to real “practice” (but sterile)
Process Logics

- apply theory to concurrency
- focus on interaction of theory and practice
- still a large breach in both

There are other theories

We will use simplest process logic: CCS
Von Neumann Architecture

Program is a mathematical function over memory state

- given a start state, can calculate solution

Assumes subservient memory, under sole control of single serial thread.

Equality – for now nebulous –

semantic equality results in same results.
Von Neumann Architecture

Program 1
\[ x := 1; \]
\[ \text{eval } x \]

Program 2
\[ x := 0; \]
\[ x := x + 1 \]
\[ \text{eval } x \]

Are models equivalent?
Von Neumann Architecture

Program 1
\[ x := 1; \]
\[ \text{eval } x \]

Program 2
\[ x := 0; \]
\[ x := x + 1 \]
\[ \text{eval } x \]

Are models equivalent: yes under Von-Neumann model

What about concurrent model?
Von Neumann Architecture

Program 1
\[ x := 1; \]
\[ \text{eval } x \]

Program 2
\[ x := 0; \]
\[ x := x + 1 \]
\[ \text{eval } x \]

Are models equivalent: yes under Von-Neumann model

What about concurrent model: no.
Concurrent architecture

Program 1
\[ x := 1; \]
\[ \text{eval } x \]

Program 2
\[ x := 0; \]
\[ x := x + 1 \]
\[ \text{eval } x \]

Assume daemon: \( x := 1; \), or concurrent operation of programs. \( x \) can be 1 or 2.

Look at results of interactions of concurrent systems

- who and when memory location \( x \) is accessed
Concurrent architectures

key: memory no longer a “slave”;
memory now 1st class agent with behavior that needs modeling.

“He who serves two masters serves none”

Think asynchronously: each model is own master.
Calculus of Communicating Systems

Milner’s CCS:
- semantic theory in which interaction and communication is central idea.
- achieves smooth mathematical treatment

Hoar’s CSP:
same primitive notion for different purpose
- the ability to derive other primitives
  - semaphores and monitors (themselves taken as primitives) from one general primitive

Both converged to same point of the pivotal nature of interaction and communication between behaviors.
Process Logics

Evidence that this notation is a pivotal one:

- serial interacting agents
- communication primitive
Other concurrency theories

- Petri nets
  - (I learned this from one of Carl Petri’s contemporaries)
  - independence (parallel) of actions
  - place transition nets / signal transition graphs

True Concurrency vs interleaving concurrency

- true concurrency
- first good theory of concurrency
  - still used today for most asynchronous modeling
Petri Nets

Benefits:

1. causality directly represented
   - virtue of places
   - preconditions

Problems:

1. Structural issue not addressed
   - results in serious drawbacks
     - not compositional operator defined
     - not able to hide actions
   - attempted to model with “Snippets” and other “warts”

2. no general theory of equality or canonical representation
Process Logics

1. Interleaving semantics
   - loose causality
     - becomes an “observational” or “existential” theory
     - (turns weakness into a strength)
     - CCS not even directly observable (due to $\tau$)

2. Direct Structural aspect
   - independent parallel “process” or “agent” set
     - each process has localized behavior
   - clear definition of “interaction” or “synchronization”
   - ability to hide non-critical detail and hierarchy

results in tractable theory which focuses on local behavior and interaction.

no theory exists that directly supports both causality and structure
Process Logics

Processes *interact*

- core is an **algebra**
  
  *various systems or branches of mathematics concerned with the properties and relationships of abstract entities manipulated in symbolic form under operations often analogous to those of arithmetic.*
  
  - everything *cannot* be done with algebra
  - still have need for **higher order logic** or *theorem proving*

- "Calculus" of communicating systems
  
  *a method of computation or calculation in a special notation (as of logic or symbolic logic)*
  
  - implies use of logic
  - temporal logic applies here
SECTION 2
Communication and concurrency are complex notations formalized in process logics.

**Concurrency:** Independence or locality of behavior

**Communication:** unifies independent models into a single system

Underlying notion of identity:

- agents: identifiable behaviors that persist in time
CCS

Systems consist of discrete actions.

Actions come in two independent classes:

1. dependency
   - actions can be independent
   - or constrained by communication or synchronization

2. observability
   - actions can be externally observed
   - actions are unobservable, but their results can be observed
     - unobservable action: $\tau$
Agents represent the current state
State to state transitions occur via actions
Hence it is convenient to write these as:

\[ P \xrightarrow{\alpha} Q \]
Notation

Agents: \( \mathcal{P} \)
Names: \( \mathcal{A} \)
CoName: \( \overline{\mathcal{A}} \)
Labels: \( \mathcal{L} \)
unobservable action: \( \tau \)
Actions: \( \text{Act} \)
Agent Expressions: \( \mathcal{E} \)

\( P, Q, \ldots \) range over \( \mathcal{P} \)
\( a, b, \ldots \) range over \( \mathcal{A} \)
\( \overline{a}, \overline{b}, \ldots \) range over \( \overline{\mathcal{A}} \)
\( \mathcal{L} = \mathcal{A} \cup \overline{\mathcal{A}} \)
\( \text{Act} = \mathcal{L} \cup \{ \tau \} \)
\( \alpha, \beta, \ldots \) range over \( \text{Act} \)
\( E, F, \ldots \) range over \( \mathcal{E} \)
\( \{ E_i : i \in I \} \)
Agent Expressions

Nil does nothing \((\sum_{i\in 0} E_i)\)

Constant \(A = P\); (infinite behavior via recursion)

prefixing \(\alpha. E\) \((\alpha \in Act)\)

Now we have the power to define simple agents:

\text{Match} = \text{strike.burn}.\text{Nil};

\text{CooCoo} = \text{tick.tock}.\text{CooCoo};
Choice

Summation $\sum_{i \in I} E_i$

Summation implements non-deterministic choice.

- interleaving parallelism

We now have ability to express more powerful agents:

C-element can now be derived from state diagram earlier:

C-element = a.b.'c.C-Element + b.a.'c.C-Element

(note: 'a is textual representation of $\overline{a}$)
Synchronization

These are the synchronizing primitives:

Composition \( E_1 \parallel E_2 \)

Restriction \( E \setminus L \) \((L \text{ should be } \mathcal{A})\)

Relabeling \( E[f] \)

\( f \) is a relabeling function mapping \( L \) to \( L \) such that

\[ f(\overline{\alpha}) = f(\alpha) \text{ and } f(\tau) = \tau \]

signal complementation \( \overline{\overline{a}} = a \)
Composition

\[ a \cdot \bar{A} \cdot \bar{c} \quad \text{c} \cdot \bar{B} \cdot \bar{b} \]

\[ A \overset{\text{def}}{=} a.A' \quad B \overset{\text{def}}{=} c.B' \]

\[ A' \overset{\text{def}}{=} \bar{c}.A \quad B' \overset{\text{def}}{=} \bar{b}.B \]

Now consider:

\[ a \cdot \bar{A} \cdot \bar{c} \quad c \cdot \bar{B} \cdot \bar{b} \]

What is the difference between \( \bar{c} \) and \( c \)?
Composition

\[
\begin{align*}
a \cdot (A) \cdot \overline{c} & \quad c \cdot (B) \cdot \overline{b} \\
A & \overset{\text{def}}{=} a.A' \\
A' & \overset{\text{def}}{=} \overline{c}.A \\
B & \overset{\text{def}}{=} c.B' \\
B' & \overset{\text{def}}{=} \overline{b}.B
\end{align*}
\]

Now consider:

\[
\begin{align*}
a \cdot (A) \cdot \overline{c} & \quad c \cdot (B) \cdot \overline{b}
\end{align*}
\]

What is the difference between \(c\) and \(\overline{c}\)?

Names and CoNames (inputs and outputs)
Composition

\[ a \cdot (A) \cdot \bar{c} \quad \quad c \cdot (B) \cdot \bar{b} \]
\[ A \overset{\text{def}}{=} a.A' \quad \quad B \overset{\text{def}}{=} c.B' \]
\[ A' \overset{\text{def}}{=} \bar{c}.A \quad \quad B' \overset{\text{def}}{=} \bar{b}.B \]

Now consider:

\[ a \cdot (A) \cdot \bar{c} \quad \quad c \cdot (B) \cdot \bar{b} \]

Can \( \bar{c} \) fire \textit{independently} in the lower graph?
Composition

\[
a \cdot (A) \cdot \overline{c} \quad \quad \quad \quad c \cdot (B) \cdot \overline{b}
\]

\[
A \overset{\text{def}}{=} a.A' \quad \quad \quad \quad B \overset{\text{def}}{=} c.B'
\]

\[
A' \overset{\text{def}}{=} \overline{c}.A \quad \quad \quad \quad B' \overset{\text{def}}{=} \overline{b}.B
\]

Now consider:

\[
a \cdot (A) \overline{c} \quad \quad c \cdot (B) \overline{b}
\]

Can \( \overline{c} \) fire *independently* in the lower graph?

**YES!**

Since \( A' \overset{\overline{c}}{\rightarrow} A \), we infer \( A' \mid B \overset{\overline{c}}{\rightarrow} A \mid B \)

This does **not** indicate communication between \( A \) and \( B \).
Composition

\[ a \cdot \overline{A} \cdot \overline{c} \quad \quad c \cdot \overline{B} \cdot \overline{b} \]

\[ A \stackrel{\text{def}}{=} a.A' \quad \quad B \stackrel{\text{def}}{=} c.B' \]

\[ A' \stackrel{\text{def}}{=} \overline{c}.A \quad \quad B' \stackrel{\text{def}}{=} \overline{b}.B \]

Now consider:

\[ a \cdot \overline{A} \cdot \overline{c} \quad \quad c \cdot \overline{B} \cdot \overline{b} \]

Can \( c \) and \( \overline{c} \) **handshake communicate** in the lower graph?
Composition

\[
\begin{align*}
  a \cdot (A) \cdot \overline{c} & \quad c \cdot (B) \cdot \overline{b} \\
  A \overset{\text{def}}{=} a.A' & \quad B \overset{\text{def}}{=} c.B' \\
  A' \overset{\text{def}}{=} \overline{c}.A & \quad B' \overset{\text{def}}{=} \overline{b}.B
\end{align*}
\]

Now consider:

\[
\begin{align*}
  a \cdot (A) \cdot \overline{c} & \quad c \cdot (B) \cdot \overline{b}
\end{align*}
\]

Can \( c \) and \( \overline{c} \) \textbf{handshake communicate} in the lower graph?

YES!

Since \( A' \overset{\overline{c}}{\rightarrow} A \), and \( B \overset{c}{\rightarrow} B' \), we infer \( A' \mid B \overset{?}{\rightarrow} A \mid B' \)
Composition

\[
a \cdot (A \cdot \overline{c}) \quad c \cdot (B \cdot \overline{b})
\]

\[
A \overset{\text{def}}{=} a.A' \quad B \overset{\text{def}}{=} c.B'
\]

\[
A' \overset{\text{def}}{=} \overline{c}.A \quad B' \overset{\text{def}}{=} \overline{b}.B
\]

Now consider:

\[
a \cdot (A \cdot \overline{c}) \quad c \cdot (B \cdot \overline{b})
\]

Since \( A' \overset{\overline{c}}{\rightarrow} A \), and \( B \overset{c}{\rightarrow} B' \), we infer \( A' \mid B \overset{?}{\rightarrow} A \mid B' \)

When we have handshake communication what is the ‘?’ action?
Composition

\[
\begin{align*}
\quad & a \cdot (A) \cdot \overline{c} \\
\quad & c \cdot (B) \cdot \overline{b} \\
A & \overset{\text{def}}{=} a.A' \\
A' & \overset{\text{def}}{=} \overline{c}.A \\
B & \overset{\text{def}}{=} c.B' \\
B' & \overset{\text{def}}{=} \overline{b}.B
\end{align*}
\]

Now consider:

\[
\begin{align*}
\quad & a \cdot (A) \cdot \overline{c} \\
\quad & c \cdot (B) \cdot \overline{b}
\end{align*}
\]

Since \( A' \overset{\overline{c}}{\rightarrow} A \), and \( B \overset{c}{\rightarrow} B' \), we infer \( A' \mid B \overset{?}{\rightarrow} A \mid B' \)

When we have handshake communication what is the ‘?’ action?
\( \tau \) – the invisible internal action.

*The \( \tau \) action has semantic properties in CCS that are significantly different than other process logics, labeled transition systems (LTS), or concurrency models.*
Composition

\[ a \cdot \overline{A} \cdot \overline{c} \quad c \cdot \overline{B} \cdot \overline{b} \]

\[ A \overset{\text{def}}{=} a.A' \quad B \overset{\text{def}}{=} c.B' \]

\[ A' \overset{\text{def}}{=} \overline{c}.A \quad B' \overset{\text{def}}{=} \overline{b}.B \]

Now consider:

\[ a \cdot \overline{A} \cdot \overline{c} \quad c \cdot \overline{B} \cdot \overline{b} \]

Can \( \overline{c} \) communicate with other agents in the system that can do the \( c \) action?
Composition

\[ a \cdot (A) \cdot \overline{c} \quad c \cdot (B) \cdot \overline{b} \]

\[ A \stackrel{\text{def}}{=} a.A' \quad B \stackrel{\text{def}}{=} c.B' \]

\[ A' \stackrel{\text{def}}{=} \overline{c}.A \quad B' \stackrel{\text{def}}{=} \overline{b}.B \]

Now consider:

\[ a \cdot (A) \cdot \overline{c} \quad c \cdot (B) \cdot \overline{b} \]

Can \( \overline{c} \) communicate with other agents in the system that can do the \( c \) action?

YES!! This is a primary means of specifying semaphores, nondeterminism, etc. in a system!
Composition

\[ a \cdot (A) \cdot \bar{c} \quad c \cdot (B) \cdot \bar{b} \]

\[ A \overset{\text{def}}{=} a.A' \quad B \overset{\text{def}}{=} c.B' \]

\[ A' \overset{\text{def}}{=} \bar{c}.A \quad B' \overset{\text{def}}{=} \bar{b}.B \]

Now consider:

\[ a \cdot (A) \cdot \bar{c} \quad c \cdot (B) \cdot \bar{b} \]

Can we **force** the communication to occur? How do we prevent the **independent** \( \bar{c} \) and \( c \) actions from occurring?
Composition

\[
\begin{align*}
    a \cdot (A) \cdot \overline{c} & \quad c \cdot (B) \cdot \overline{b} \\
    A & \overset{\text{def}}{=} a \cdot A' \\
    A' & \overset{\text{def}}{=} \overline{c} \cdot A \\
    B & \overset{\text{def}}{=} c \cdot B' \\
    B' & \overset{\text{def}}{=} \overline{b} \cdot B
\end{align*}
\]

Now consider:

\[
\begin{align*}
    a \cdot (A) \cdot \overline{c} & \quad c \cdot (B) \cdot \overline{b}
\end{align*}
\]

Can we **force** the communication to occur? How do we prevent the independent \(\overline{c}\) and \(c\) actions from occurring?

**YES!** – this is the purpose of the **restriction** operator! The operator \((A \mid B) \setminus \{c\}\) will restrict the \(c\) and \(\overline{c}\) actions from occurring in the composed process.
Transitional Semantics

A labeled transition system \( \text{LTS} = (S, T, \{\overset{t}{\rightarrow}: t \in T\}) \)

\( S \): state set
\( T \): Transition label set

Transition relation: \( \overset{t}{\rightarrow} \subseteq S \times S \ \forall t \in T \)

Also:

\( S ::= \mathcal{E} \)
\( T ::= \text{Act} \)

Semantics for agent expressions \( \mathcal{E} \) consist in the definition of each transition relation over \( \mathcal{E} \).
Simple Examples

Sender → (medium) → Receiver

- sender can send data at any time
- when ether not empty, receiver can accept at any time

Medium: ether
  non-order-preserving
  bounded buffer
  buffer
  shared memory
  ...

Must be able to represent them all.

Just like Von-Neumann example and parallel computer – the medium just like the memory can have its own arbitrary behavior, and thus can be represented as an independent agent!
Bounded FIFO

FIFO = in(x).FIFO'(x);
FIFO'(x) = 'out(x).FIFO;

Equivalent definition:
FIFO = in(x).'out(x).FIFO;

What of $F \circ F \circ F$? (composition?)

Exercise 1, page 18 of Milner
SECTION 3
Review

\[ E ::= \]

- \( A \) \hspace{1cm} \text{constant}
- \( \alpha . E \) \hspace{1cm} \text{prefixing}
- \( \sum_{i \in I} E_i \) \hspace{1cm} \text{summation}
- \( E_1 | E_2 \) \hspace{1cm} \text{composition}
- \( E[f] \) \hspace{1cm} \text{relabeling}
- \( E \setminus L \) \hspace{1cm} \text{restriction}

\[ \text{LTS} = (S, T, \{ t \mapsto t \in T \}) \]

In composition, a name and coname interact to form a single indivisible communication action \( \tau \).
Derivation Tree

For the process:

\[ a \xrightarrow{\text{A}} b \]

we can create the derivation tree:

```
(\text{A} | \text{B}) \{c\}
  \downarrow a
  (\text{A}' | \text{B}) \{c\}
  \downarrow \tau
  (\text{A} | \text{B}') \{c\}
  \downarrow \overline{b}
  (\text{A} | \text{B}) \{c\}
  \downarrow a
  (\text{A}' | \text{B}) \{c\}
  \downarrow \overline{b}
  (\text{A}' | \text{B}) \{c\}
  \vdots
  (\text{A}' | \text{B}') \{c\}
```

...
Derivation Tree

For the process:

\[ a \circ A \rightarrow B \cdot \bar{b} \]

The cyclic nature allows us to represent this behavior as a transition graph:

\[ \begin{align*}
(A | B) \setminus \{c\} & \xrightarrow{\bar{b}} (A | B') \setminus \{c\} & \xrightarrow{a} (A' | B') \setminus \{c\} \\
(A' | B) \setminus \{c\} & \xrightarrow{a} (A' | B') \setminus \{c\} & \xrightarrow{\bar{b}} (A | B) \setminus \{c\}
\end{align*} \]
Internal Actions

The internal action $\tau$

1. has no complement
2. cannot communicate with other actions
3. is not directly observable

We want to define systems as equivalent if they can perform the same pattern of external actions.

This results in the ability to abstract:

Should $P \xrightarrow{\tau} P_1 \xrightarrow{\tau} \ldots \xrightarrow{\tau} P_n$ be equal to $P \xrightarrow{\tau} P_n$??
Internal Actions

The internal action $\tau$

1. has no complement
2. cannot communicate with other actions
3. is not directly observable

We want to define systems as equivalent if they can perform the same pattern of *external* actions.

This results in the ability to abstract:

Should $P \xrightarrow{\tau} P_1 \xrightarrow{\tau} \cdots \xrightarrow{\tau} P_n$

be equal to $P \xrightarrow{\tau} P_n$??

YES!! We will define the transitional semantics and rules that show this to be the case.
Transitional Semantics

Transitional semantics of
LTS = (S, T, {t →: t ∈ T})

These come in form of:
RULE \texttt{name} \rightarrow \texttt{Act}

Top of the bar is the \textbf{hypothesis}
Bottom of bar is the \textbf{conclusion}

\begin{eqnarray*}
\text{Act} & \xrightarrow{\alpha} & \text{Prefixing} \\
\alpha \cdot E & \rightarrow & E
\end{eqnarray*}
Transitional Semantics

\[
\begin{align*}
\text{Sum}_j & \quad E_j \xrightarrow{\alpha} E'_j \\
\text{Summation} & \quad \sum_{i \in I} E_i \xrightarrow{\alpha} E'_j \\
\end{align*}
\]

- case \( I = 0 \), result is \( 0 \) or \( \text{NIL} \)
- case \( I = \{1, 2\} \)
  \( \sum_{i \in \{1,2\}} E_i \) is written \( E_1 + E_2 \) and has transition rules

\[
\begin{align*}
E_1 \xrightarrow{\alpha} E'_1 \\
E_1 + E_2 \xrightarrow{\alpha} E'_1 \\
\text{and} \\
E_2 \xrightarrow{\alpha} E'_2 \\
E_1 + E_2 \xrightarrow{\alpha} E'_2
\end{align*}
\]
Example

C-element defined as:

\[ C = a.b.'c.C + b.a.'c.C; \]

rules are

\[ a.b.'c.C \xrightarrow{a} b.'c.C \]

\[ a.b.'c.C + b.a.'c.C \xrightarrow{a} b.'c.C \]

and

\[ b.a.'c.C \xrightarrow{b} a.'c.C \]

\[ a.b.'c.C + b.a.'c.C \xrightarrow{b} a.'c.C \]
Names joined to corresponding conames

$E_1|E_2$ has three rules:
Transitional Semantics

\[ E_1 \xrightarrow{\alpha} E'_1 \]

\[ E_1 \mid E_2 \xrightarrow{\alpha} E'_1 \mid E_2 \]

\[ E_2 \xrightarrow{\alpha} E'_2 \]

\[ E_1 \mid E_2 \xrightarrow{\alpha} E'_1 \mid E'_2 \]

\[ E_1 \xrightarrow{\bar{l}} E'_1 \quad E_2 \xrightarrow{\bar{l}} E'_2 \]

\[ E_1 \mid E_2 \xrightarrow{\tau} E'_1 \mid E'_2 \]

\( l \in \mathcal{L} \)

if \( l \) is \( \bar{b} \) then \( \bar{\bar{l}} \) is \( \bar{b} = b \)

if \( l \) is \( c \) then \( \bar{\bar{l}} \) is \( \bar{c} \)
Transitional Semantics

\( \tau \) is the unobservable internal action

- \( \tau \) is neither a name or coname
- \( \bar{\tau} \) is not a well-formed action expression

Note:

- In Com\(_3\) we get \( \tau \) whether \( l \) or \( \bar{l} \) give rise to the communication.
- We cannot tell from \( \tau \) exactly what goes on inside \( E_1 \mid E_2 \)
- Likewise, we cannot differentiate between the \( b \) and \( c \) tau transitions
  - unless it creates a difference in externally observable behavior
- only single internal transition label necessary
- most (all?) other languages use a hiding semantics!
Transition Semantics

SORTS:

Definition: for any \( L \subseteq L \), if the actions of \( P \) and all its derivatives lie in \( L \cup \{ \tau \} \) then we say \( P \) has sort \( L \), or \( L \) is a sort of \( P \), and write \( P:L \).

Proposition: For every \( E \) and \( L \), \( L \) is a sort of \( E \) if and only if, whenever \( E \xrightarrow{\alpha} E' \), then

1. \( \alpha \in L \cup \{ \tau \} \)

2. \( L \) is a sort of \( E' \)
Transitional Semantics

For $E$ with sort $K$ and $F$ with sort $L$
(This is used for hardware modeling and broadcast communication)

Conj$_1$

- $E \xrightarrow{\alpha} E' \quad \alpha \notin L$
- $E \mid F \xrightarrow{\alpha} E' \mid F$

Conj$_2$

- $F \xrightarrow{\alpha} F' \quad \alpha \notin K$
- $E \mid F \xrightarrow{\alpha} E \mid F'$

Conj$_3$

- $E \xrightarrow{\bar{l}} E' \quad F \xrightarrow{l} F' \quad l \in K \cap L$
- $E \mid F \xrightarrow{\tau} E' \mid F'$

(We can allow $\tau$ to be $\bar{l}$ for circuit semantics, and can allow $l$ to communicate with $l$ as shared inputs.)
Relabeling

$f$ is relabeling function, so $f : \text{Act} \rightarrow \text{Act}$

- $f(\tau) = \tau$
- $f(l) \in \mathcal{L}$ when $l \in \mathcal{L}$
- $f(l) = \overline{f(l)} \ \forall \ l \in \mathcal{L}$

\[
\begin{array}{c}
E \xrightarrow{\alpha} E' \\
\hline
\text{Rel}
\end{array}
\]

\[
E[f] \xrightarrow{f(\alpha)} E'[f]
\]
Relabeling

Notation:
when \( f(l_i) = l'_i. \ (i = 1, \ldots, n) \)
\( f(l) = l \) if \( l \neq l_1, \ldots, l_n \)
written \( E[f] \) as \( E[l'_1/l_1, \ldots, l'_n/l_n] \)
Relabeling

Problems exist without restriction:

FIFO = in.'out.FIFO

♣:

FIFO | FIFO

♠:

FIFO[mid/out] | FIFO[mid/in]

Draw transition graph for ♣

Draw derivation tree for ♠

Note problem of independent actions!
Restriction

$L \subseteq \mathcal{L}$

\[
\begin{array}{c}
E \xrightarrow{\alpha} E' \\
\hline
E \setminus L \xrightarrow{\alpha} E' \setminus L
\end{array}
\]

$(\alpha, \overline{\alpha} \notin L)$

- $E \setminus L$ has the same $\tau$ transitions as $E$ since $\tau \notin \mathcal{L}$
- Syntax of some tools assumes $L \notin \bar{\mathcal{A}}$, but $L \in \mathcal{A}$
Hiding

Hiding is the semantics for internal signals for *most* process logics and LTS

$L \subseteq L$

\[ E \xrightarrow{\alpha} E' \]

\[ E/L \xrightarrow{\alpha} E'/L \quad (\alpha, \bar{\alpha} \notin L) \]

\[ E \xrightarrow{l} E' \]

\[ E/L \rightarrow E'/L \quad (l \lor \bar{l} \in L) \]

Does this result in $E$ and $E'$ being equivalent?
Hiding

Hiding is the semantics for internal signals for most process logics and LTS

\[ L \subseteq L \]

\[
\begin{align*}
\text{Hid}_1 & \quad E \overset{\alpha}{\rightarrow} E' \\
& \quad \quad \quad \quad \quad \quad \quad \quad (\alpha, \overline{\alpha} \not\in L) \\
E/L & \overset{\alpha}{\rightarrow} E'/L
\end{align*}
\]

\[
\begin{align*}
\text{Hid}_2 & \quad E \overset{l}{\rightarrow} E' \\
& \quad \quad \quad \quad \quad \quad \quad \quad (l \lor \overline{l} \in L) \\
E/L & \overset{l}{\rightarrow} E'/L
\end{align*}
\]

Does this result in \( E \) and \( E' \) being equivalent?

YES
Example

Now try this FIFO:

FIFO = in.'out.FIFO

(FIFO[mid/out] | FIFO[mid/in]) \{ mid \}

Make transition Graph

Make Derivation Tree
Examples

1. inverter
2. buffer
3. toggle
4. fork
5. merge
6. semaphore
7. mutex element