Concurrency Theory

Lecture 8: Bisimilarity and Testing

Stephan Mennicke
Knowledge-Based Systems Group

June 7, 2023

Recap: CCS

$\mathcal{N} = \{a, b, c, \ldots\}$ ...set of names ($\tau \notin \mathcal{N}$)

$\overline{\mathcal{N}} = \{\overline{\alpha} \mid \alpha \in \mathcal{N}\}$ ...set of conames

$Act = \mathcal{N} \cup \overline{\mathcal{N}} \cup \{\tau\}$ (note, there is no $\overline{\tau}$ and for $\alpha \in Act \setminus \{\tau\}$, $\overline{\overline{\alpha}} = \alpha$)

The set of (CCS) processes *Pr* is defined by

$$P \quad ::= \quad \mathbf{0} \;\Big|\; \mu.P \;\Big|\; P + P \;\Big|\; P \mid P \;\Big|\; (\nu a)(P) \;\Big|\; K$$

where $\mu \in Act$, $a \in \mathcal{N}$, and $K \in \mathcal{K}$.

Define the language CCS parameterized over Act, $\mathcal{K}$, and $\mathcal{T}_{\mathcal{K}} \subseteq \mathcal{K} \times Act \times Pr$.

$$\mathsf{CCS}(Act, \mathcal{K}, \mathcal{T}_{\mathcal{K}})$$

Recap: SOS of CCS

$\mathsf{CCS}(Act, \mathcal{K}, \mathcal{T}_\mathcal{K})$ specifies an LTS $(Pr, Act, \rightarrow \cup \mathcal{T}_\mathcal{K})$ where $\rightarrow \subseteq (Pr \setminus \mathcal{K}) \times Act \times Pr$ is the smallest relation satisfying the following rules:

$$\text{(Pref)}\ \frac{}{\mu.P \xrightarrow{\mu} P}$$

$$\text{(SumL)}\ \frac{P \xrightarrow{\mu} P'}{P + Q \xrightarrow{\mu} P'} \qquad \text{(SumR)}\ \frac{Q \xrightarrow{\mu} Q'}{P + Q \xrightarrow{\mu} Q'}$$

$$\text{(ParL)}\ \frac{P \xrightarrow{\mu} P'}{P \mid Q \xrightarrow{\mu} P' \mid Q} \qquad \text{(ParR)}\ \frac{Q \xrightarrow{\mu} Q'}{P \mid Q \xrightarrow{\mu} P \mid Q'}$$

$$\text{(Com)}\ \frac{P \xrightarrow{\mu} P' \quad Q \xrightarrow{\overline{\mu}} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'} \qquad \text{(Res)}\ \frac{P \xrightarrow{\mu} P'}{(\nu a)\,(P) \xrightarrow{\mu} (\nu a)\,(P')}\ \text{if } a \notin \{\mu, \overline{\mu}\}$$

What about Interaction? Testing (1/2)

- Two processes are *equivalent* if no *experiment* distinguishes them
- Experiment = test, a pattern of demands on the process
- Observer reports about *success* or *failure* of the test, depending on the process behavior
- Our goal: set up a testing scenario such that the distinguishing power of tests is exactly that of bisimilarity

What about Interaction? Testing (2/2)

- As before, we consider a single LTS $(Pr, Act, \rightarrow)$.
- Additionally, we'll assume image-finiteness for the transition system.
- Tests are objects T that are performed on a process as a form of experiment.
- We use $\top$ to indicate success and $\bot$ for lack of success.
- Because of nondeterminism, different runs may produce different results.
- For tests T and processes P we, thus, look at observations

$$\mathcal{O}(T, P) \subseteq \{\top, \bot\}$$

- Two processes P and Q are *behaviorally equivalent* iff $\mathcal{O}(T, P) = \mathcal{O}(T, Q)$ for all tests T.

Testing: Syntax and Semantics

A test T is an expression of the following grammar:

$$T \quad ::= \quad \mathsf{SUCC} \mid \mathsf{FAIL} \mid \mu.T \mid \tilde{\mu}.T \mid T \wedge T \mid T \vee T \mid \forall T \mid \exists T$$

For an arbitrary process P and test T, define the observations admitted by P through T as:

$$\begin{aligned}
\mathcal{O}(\mathsf{SUCC}, P) &= \{\top\} \\
\mathcal{O}(\mathsf{FAIL}, P) &= \{\bot\} \\
\mathcal{O}(\mu.T, P) &= \begin{cases} \{\bot\} & \text{if } P \stackrel{\mu}{\not\to} \\ \bigcup\{\mathcal{O}(T, P') \mid P \xrightarrow{\mu} P'\} & \text{otherwise.} \end{cases} \\
\mathcal{O}(\tilde{\mu}.T, P) &= \begin{cases} \{\top\} & \text{if } P \stackrel{\mu}{\not\to} \\ \bigcup\{\mathcal{O}(T, P') \mid P \xrightarrow{\mu} P'\} & \text{otherwise.} \end{cases} \\
\mathcal{O}(T_1 \wedge T_2, P) &= \mathcal{O}(T_1, P) \wedge^\star \mathcal{O}(T_2, P) \\
\mathcal{O}(T_1 \vee T_2, P) &= \mathcal{O}(T_1, P) \vee^\star \mathcal{O}(T_2, P)
\end{aligned}$$

Testing: Syntax and Semantics

$$T \quad ::= \quad \mathsf{SUCC} \;\big|\; \mathsf{FAIL} \;\big|\; a.T \;\big|\; \tilde{a}.T \;\big|\; T \wedge T \;\big|\; T \vee T \;\big|\; \forall T \;\big|\; \exists T$$

$$\begin{aligned}
\mathcal{O}(\mathsf{SUCC}, P) &= \{\top\} \\
\mathcal{O}(\mathsf{FAIL}, P) &= \{\bot\} \\
\mathcal{O}(a.T, P) &= \begin{cases} \{\bot\} & \text{if } P \stackrel{a}{\not\to} \\ \bigcup\{\mathcal{O}(T, P') \mid P \stackrel{a}{\to} P'\} & \text{otherwise.} \end{cases} \\
\mathcal{O}(\tilde{a}.T, P) &= \begin{cases} \{\top\} & \text{if } P \stackrel{a}{\not\to} \\ \bigcup\{\mathcal{O}(T, P') \mid P \stackrel{a}{\to} P'\} & \text{otherwise.} \end{cases} \\
\mathcal{O}(T_1 \wedge T_2, P) &= \mathcal{O}(T_1, P) \wedge^\star \mathcal{O}(T_2, P) \\
\mathcal{O}(T_1 \vee T_2, P) &= \mathcal{O}(T_1, P) \vee^\star \mathcal{O}(T_2, P) \\
\mathcal{O}(\forall T, P) &= \begin{cases} \{\bot\} & \text{if } \bot \in \mathcal{O}(T, P) \\ \{\top\} & \text{otherwise} \end{cases} \\
\mathcal{O}(\exists T, P) &= \begin{cases} \{\top\} & \text{if } \top \in \mathcal{O}(T, P) \\ \{\bot\} & \text{otherwise} \end{cases}
\end{aligned}$$

Properties of Tests and Observation (1/)

Theorem 1
Every test T has an inverse test $\overline{T}$, such that for all processes P,

1. $\bot \in \mathcal{O}(T, P)$ *if, and only if,* $\top \in \mathcal{O}(\overline{T}, P)$ *and*
2. $\top \in \mathcal{O}(T, P)$ *if, and only if,* $\bot \in \mathcal{O}(\overline{T}, P)$.

Proof (of 1): Define $\overline{T}$ by

$$
\begin{array}{rclcrcl}
\overline{\mathsf{SUCC}} & = & \mathsf{FAIL} & \qquad & \overline{\mathsf{FAIL}} & = & \mathsf{SUCC} \\
\overline{a.T'} & = & \tilde{a}.\overline{T'} & & \overline{\tilde{a}.T'} & = & a.\overline{T'} \\
\overline{T_1 \wedge T_2} & = & \overline{T_1} \vee \overline{T_2} & & \overline{T_1 \vee T_2} & = & \overline{T_1} \wedge \overline{T_2} \\
\overline{\exists T'} & = & \forall \overline{T'} & & \overline{\forall T'} & = & \exists \overline{T'}
\end{array}
$$

Proof by induction on the structure of T. Let P be a process.

Base: $T = \mathsf{FAIL}$. Then $\mathcal{O}(T, P) = \{\bot\}$ and $\mathcal{O}(\overline{T}, P) = \mathcal{O}(\mathsf{SUCC}, P) = \{\top\}$.

Properties of Tests and Observations (2/)

$$
\begin{array}{rclcrcl}
\overline{\mathsf{SUCC}} & = & \mathsf{FAIL} & \quad & \overline{\mathsf{FAIL}} & = & \mathsf{SUCC} \\
\overline{a.T'} & = & \tilde{a}.\overline{T'} & & \overline{\tilde{a}.T'} & = & a.\overline{T'} \\
\overline{T_1 \wedge T_2} & = & \overline{T_1} \vee \overline{T_2} & & \overline{T_1 \vee T_2} & = & \overline{T_1} \wedge \overline{T_2} \\
\overline{\exists T'} & = & \forall \overline{T'} & & \overline{\forall T'} & = & \exists \overline{T'}
\end{array}
$$

Step: By case distinction.

- $T = T_1 \wedge T_2$: $\bot \in \mathcal{O}(T, P)$ iff $\bot \in \mathcal{O}(T_1, P)$ or $\bot \in \mathcal{O}(T_2, P)$ iff(IH) $\top \in \mathcal{O}(\overline{T_1}, P)$ or $\top \in \mathcal{O}(\overline{T_2}, P)$ iff $\top \in \mathcal{O}(\overline{T_1} \vee \overline{T_2}, P)$ iff $\top \in \mathcal{O}(\overline{T}, P)$
- $T = T_1 \vee T_2$: $\bot \in \mathcal{O}(T, P)$ iff $\bot \in \mathcal{O}(T_1, P)$ and $\bot \in \mathcal{O}(T_2, P)$ iff(IH) $\top \in \mathcal{O}(\overline{T_1}, P)$ and $\top \in \mathcal{O}(\overline{T_2}, P)$ iff $\top \in \mathcal{O}(\overline{T_1} \wedge \overline{T_2}, P)$ iff $\top \in \mathcal{O}(\overline{T}, P)$

Properties of Tests and Observations (3/)

$$\begin{array}{rclcrcl}
\overline{\mathsf{SUCC}} & = & \mathsf{FAIL} & \quad & \overline{\mathsf{FAIL}} & = & \mathsf{SUCC} \\
\overline{a.T'} & = & \tilde{a}.\overline{T'} & & \overline{\tilde{a}.T'} & = & a.\overline{T'} \\
\overline{T_1 \wedge T_2} & = & \overline{T_1} \vee \overline{T_2} & & \overline{T_1 \vee T_2} & = & \overline{T_1} \wedge \overline{T_2} \\
\overline{\exists T'} & = & \forall \overline{T'} & & \overline{\forall T'} & = & \exists \overline{T'}
\end{array}$$

Step: By case distinction.

- $T = \exists T'$: $\bot \in \mathcal{O}(T, P)$ iff $\mathcal{O}(T', P) = \{\bot\}$ iff(IH) $\mathcal{O}(\overline{T'}, P) = \{\top\}$ iff $\top \in \mathcal{O}(\forall \overline{T'}, P)$ iff $\top \in \mathcal{O}(\overline{T}, P)$.
- $T = \forall T'$: $\bot \in \mathcal{O}(T, P)$ iff $\bot \in \mathcal{O}(T', P)$ iff(IH) $\top \in \mathcal{O}(\overline{T'}, P)$ iff $\top \in \mathcal{O}(\exists \overline{T'}, P)$ iff $\top \in \mathcal{O}(\overline{T}, P)$.

Properties of Tests and Observations (4/)

$$\begin{array}{rclcrcl} \overline{\mathsf{SUCC}} & = & \mathsf{FAIL} & & \overline{\mathsf{FAIL}} & = & \mathsf{SUCC} \\ \overline{a.T'} & = & \tilde{a}.\overline{T'} & & \overline{\tilde{a}.T'} & = & a.\overline{T'} \\ \overline{T_1 \wedge T_2} & = & \overline{T_1} \vee \overline{T_2} & & \overline{T_1 \vee T_2} & = & \overline{T_1} \wedge \overline{T_2} \\ \overline{\exists T'} & = & \forall \overline{T'} & & \overline{\forall T'} & = & \exists \overline{T'} \end{array}$$

Step (cont'd): By case distinction.

- $T = a.T'$: $\bot \in \mathcal{O}(T, P)$ iff (a) $P \stackrel{a}{\not\rightarrow}$ or (b) $\bot \in \mathcal{O}(T', P')$ for some P' with $P \stackrel{a}{\rightarrow} P'$. In case (a), $\mathcal{O}(\tilde{a}.\overline{T'}, P) = \{\top\}$. In case (b), $\top \in \mathcal{O}(\overline{T'}, P')$ by IH. Hence, $\top \in \mathcal{O}(\tilde{a}.\overline{T'}, P)$ by the arguments for (a) and (b).
- $T = \tilde{a}.T'$: $\bot \in \mathcal{O}(T, P)$ iff $P \stackrel{a}{\rightarrow} P'$ (for some P') and $\bot \in \mathcal{O}(T', P')$ iff $\top \in \mathcal{O}(\overline{T'}, P')$ iff $\top \in \mathcal{O}(a.\overline{T'}, P)$ iff $\top \in \mathcal{O}(\overline{T}, P)$.

□

Properties of Tests and Observation (5/5)

Definition 2
$P \sim_T Q$ if, and only if, $\mathcal{O}(T, P) = \mathcal{O}(T, Q)$ for all tests T.

Theorem 3
If $P \not\sim_T Q$, then there is a test case T, such that $\mathcal{O}(T, P) = \{\bot\}$ and $\mathcal{O}(T, Q) = \{\top\}$.

Proof: Since $P \not\sim_T Q$, there is at least one test case T_0 with $\mathcal{O}(T_0, P) \neq \mathcal{O}(T_0, Q)$.
Transform T_0 into the required T by the following procedure:

1. If $\mathcal{O}(T_0, Q) = \{\top\}$, set $T = \forall T_0$. If $\mathcal{O}(T_0, Q) = \{\bot\}$, set $\mathcal{O}(\forall \overline{T_0})$.
2. Otherwise, if $\mathcal{O}(T_0, P) = \{\bot\}$, set $T = \exists T_0$ and if $\mathcal{O}(T_0, P) = \{\top\}$, set $T = \exists \overline{T_0}$.

$\square$

Theorem 4
$\leftrightarrows = \sim_T$ *on image-finite processes.*

Relationship to Modal Logic (1/3)

Hennessy-Milner Logic (HML) is the model logic formed by the following grammar:

$$\varphi \quad ::= \quad \mathit{true} \;\Big|\; \mathit{false} \;\Big|\; \varphi \wedge \varphi \;\Big|\; \varphi \vee \varphi \;\Big|\; [\mu]\,\varphi \;\Big|\; \langle\mu\rangle\,\varphi$$

A process P satisfies an HML formula φ, denoted $P \models \varphi$, iff

- $\varphi = \mathit{true}$;
- $\varphi = \psi_1 \wedge \psi_2$, and $P \models \psi_1$ and $P \models \psi_2$;
- $\varphi = \psi_1 \vee \psi_2$, and $P \models \psi_1$ or $P \models \psi_2$;
- $\varphi = [\mu]\,\psi$ and for all P' with $P \xrightarrow{\mu} P'$, $P' \models \psi$;
- $\varphi = \langle\mu\rangle\,\psi$ and there is a P' with $P \xrightarrow{\mu} P'$ and $P' \models \psi$.

Relationship to Modal Logic (2/3)

Hennessy-Milner Logic (HML) is the model logic formed by the following grammar:

$$\varphi \quad ::= \quad \mathit{true} \;\Big|\; \mathit{false} \;\Big|\; \varphi \wedge \varphi \;\Big|\; \varphi \vee \varphi \;\Big|\; [\mu]\,\varphi \;\Big|\; \langle\mu\rangle\,\varphi$$

Define a test in our framework from every HML formula via structural induction:

- $[\![\mathit{true}]\!] = \mathrm{SUCC}$ and $[\![\mathit{false}]\!] = \mathrm{FAIL}$;
- $[\![\psi_1 \wedge \psi_2]\!] = [\![\psi_1]\!] \wedge [\![\psi_2]\!]$ and $[\![\psi_1 \vee \psi_2]\!] = [\![\psi_1]\!] \vee [\![\psi_2]\!]$;
- $[\![[\mu]\,\psi]\!] = \forall\mu.\,[\![\psi]\!]$ and $[\![\langle\mu\rangle\,\psi]\!] = \exists\mu.\,[\![\psi]\!]$.

Relationship to Modal Logic (3/3)

- $[\![true]\!] = \text{SUCC}$ and $[\![false]\!] = \text{FAIL}$;
- $[\![\psi_1 \wedge \psi_2]\!] = [\![\psi_1]\!] \wedge [\![\psi_2]\!]$ and $[\![\psi_1 \vee \psi_2]\!] = [\![\psi_1]\!] \vee [\![\psi_2]\!]$;
- $[\![[\mu]\, \psi]\!] = \forall\mu.\, [\![\psi]\!]$ and $[\![\langle\mu\rangle\, \psi]\!] = \exists\mu.\, [\![\psi]\!]$.

Theorem 5
For every HML formula φ and process P,

1. $P \models \varphi$ *iff* $\mathcal{O}([\![\varphi]\!], P) = \{\top\}$;
2. $P \not\models \varphi$ *iff* $\mathcal{O}([\![\varphi]\!], P) = \{\bot\}$.

Two processes P and Q are HML-equivalent, denoted $P \sim_{\mathsf{HML}} Q$, iff for all HML formulae φ, $P \models \varphi$ iff $Q \models \varphi$.

Theorem 6 (Hennessy-Milner Theorem)
On image-finite processes, $\sim_{\mathsf{HML}}$ and $\leftrightarroweq$ coincide.

What about (Completed) Traces?

The Hennessy-Milner Logic:

$$\varphi \quad ::= \quad \mathit{true} \;\Big|\; \mathit{false} \;\Big|\; \varphi \wedge \varphi \;\Big|\; \varphi \vee \varphi \;\Big|\; [\mu]\,\varphi \;\Big|\; \langle\mu\rangle\,\varphi$$

The Trace Logic:

$$\varphi \quad ::= \quad \mathit{true} \;\Big|\; \langle\mu\rangle\,\varphi$$

The Completed Trace Logic:

$$\varphi \quad ::= \quad \mathit{true} \;\Big|\; \langle\mu\rangle\,\varphi \;\Big|\; [Act]\,\mathit{false}$$

Summary & Outlook

- Tests and logical formulae characterize bisimilarity
- They give insights in what is needed to distinguish processes for a certain equivalence relation

Next:

- Alternative model: Carl Adam Petri and his Nets
- What is decidable about Petri nets?
- Enhancing CCS: the π-calculus