Concurrency Theory

Lecture 3: Hennessy-Milner Logic

Joost-Pieter Katoen Thomas Noll

Lehrstuhl für Informatik 2
(Software Modeling and Verification)

RWTH AACHEN UNIVERSITY

{katoen,noll}@cs.rwth-aachen.de

http://www-i2.informatik.rwth-aachen.de/i2/ct13/

Winter Semester 2013/14

Written Exams in Concurrency Theory

1. Friday, 21.02.2014, 11:30–14:00, AH 2
2. Tuesday, 25.03.2014, 10:00–12:30, AH 1

Online registration via CampusOffice is enabled.

Wanted: Student Assistant

D-MILS
DISTRIBUTED MILS FOR DEPENDABLE INFORMATION AND COMMUNICATION INFRASTRUCTURES

- D-MILS research project (http://www.d-mils.org/)
  - architectural specification of secure systems
  - modular high-assurance platform
  - framework for the certification of systems
  - basis: MILS-AADL specification language
- Task: implementation of compiler frontend
  - parser
  - semantic checker
  - based on ANTLR 3 definition of SLIM specification language (COMPASS project)
  - estimated effort: 10 h/week

Outline

Syntax of CCS I

Definition (Syntax of CCS)

- Let A be a set of (action) names.
- $\overline{A} := \{\overline{a} \mid a \in A\}$ denotes the set of co-names.
- $Act := A \cup \overline{A} \cup \{\tau\}$ is the set of actions where τ denotes the silent (or: unobservable) action.
- Let Pid be a set of process identifiers.
- The set Prc of process expressions is defined by the following syntax:

$$\begin{array}{rcll} P & ::= & \mathsf{nil} & \text{(inaction)} \\ & \mid & \alpha.P & \text{(prefixing)} \\ & \mid & P_1 + P_2 & \text{(choice)} \\ & \mid & P_1 \parallel P_2 & \text{(parallel composition)} \\ & \mid & P \setminus L & \text{(restriction)} \\ & \mid & P[f] & \text{(relabelling)} \\ & \mid & C & \text{(process call)} \end{array}$$

where $\alpha \in Act$, $L \subseteq A$, $C \in Pid$, and $f : Act \to Act$ such that $f(\tau) = \tau$ and $f(\overline{a}) = \overline{f(a)}$ for each $a \in A$.

Syntax of CCS II

Definition (continued)

- A (recursive) process definition is an equation system of the form

$$(C_i = P_i \mid 1 \leq i \leq k)$$

  where $k \geq 1$, $C_i \in Pid$ (pairwise distinct), and $P_i \in Prc$ (with process identifiers from $\{C_1, \ldots, C_k\}$).

Notational Conventions:

- $\overline{\overline{a}}$ means a
- $\sum_{i=1}^{n} P_i$ ($n \in \mathbb{N}$) means $P_1 + \ldots + P_n$ (where $\sum_{i=1}^{0} P_i := \mathrm{nil}$)
- $P \setminus a$ abbreviates $P \setminus \{a\}$
- $[a_1 \mapsto b_1, \ldots, a_n \mapsto b_n]$ stands for $f : Act \to Act$ with $f(a_i) = b_i$ ($i \in [n]$) and $f(\alpha) = \alpha$ otherwise
- restriction and relabelling bind stronger than prefixing, prefixing stronger than composition, composition stronger than choice:

$$P \setminus a + b.Q \parallel R \quad \text{means} \quad (P \setminus a) + ((b.Q) \parallel R)$$

Labelled Transition Systems

Goal: represent behaviour of system by (infinite) graph

- nodes = system states
- edges = transitions between states

Definition (Labelled transition system)

A (Act-)labelled transition system (LTS) is a triple $(S, Act, \longrightarrow)$ consisting of

- a set S of states
- a set Act of (action) labels
- a transition relation $\longrightarrow \subseteq S \times Act \times S$

For $(s, \alpha, s') \in \longrightarrow$ we write $s \xrightarrow{\alpha} s'$. An LTS is called finite if S is so.

Remarks:

- sometimes an initial state $s_0 \in S$ is distinguished ("$LTS(s_0)$")
- (finite) LTSs correspond to (finite) automata without final states

Semantics of CCS I

Definition (Semantics of CCS)

A process definition $(C_i = P_i \mid 1 \leq i \leq k)$ determines the LTS $(Prc, Act, \longrightarrow)$ whose transitions can be inferred from the following rules ($P, P', Q, Q' \in Prc$, $\alpha \in Act$, $\lambda \in A \cup \overline{A}$, $a \in A$):

$$\text{(Act)}\,\frac{}{\alpha.P \xrightarrow{\alpha} P}$$

$$\text{(Sum}_1\text{)}\,\frac{P \xrightarrow{\alpha} P'}{P + Q \xrightarrow{\alpha} P'} \qquad \text{(Sum}_2\text{)}\,\frac{Q \xrightarrow{\alpha} Q'}{P + Q \xrightarrow{\alpha} Q'}$$

$$\text{(Par}_1\text{)}\,\frac{P \xrightarrow{\alpha} P'}{P \parallel Q \xrightarrow{\alpha} P' \parallel Q} \qquad \text{(Par}_2\text{)}\,\frac{Q \xrightarrow{\alpha} Q'}{P \parallel Q \xrightarrow{\alpha} P \parallel Q'}$$

$$\text{(Com)}\,\frac{P \xrightarrow{\lambda} P' \quad Q \xrightarrow{\overline{\lambda}} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'} \qquad \text{(Res)}\,\frac{P \xrightarrow{\alpha} P' \quad (\alpha, \overline{\alpha} \notin L)}{P \setminus L \xrightarrow{\alpha} P' \setminus L}$$

$$\text{(Rel)}\,\frac{P \xrightarrow{\alpha} P'}{P[f] \xrightarrow{f(\alpha)} P'[f]} \qquad \text{(Call)}\,\frac{P \xrightarrow{\alpha} P' \quad (C = P)}{C \xrightarrow{\alpha} P'}$$

Semantics of CCS II

Example

Parallel two-place buffer: $B_{\|} = (B[f] \parallel B[g]) \setminus com$
$B = in.\overline{out}.B$

where $f := [out \mapsto com]$ and $g := [in \mapsto com]$

$$\begin{tikzcd}
{} \arrow[r] & \boxed{B_{\|}} \arrow[d, "in"] & & \boxed{(B[f] \parallel B[g]) \setminus com} \arrow[dll, "in"] & \text{empty} \\
& \boxed{((\overline{out}.B)[f] \parallel B[g]) \setminus com} \arrow[rr, "\tau"] & & \boxed{(B[f] \parallel (\overline{out}.B)[g]) \setminus com} \arrow[u, "\overline{out}"] \arrow[dl, "in"] & \text{1 entry} \\
& & \boxed{((\overline{out}.B)[f] \parallel (\overline{out}.B)[g]) \setminus com} \arrow[ul, "\overline{out}"] & & \text{full}
\end{tikzcd}$$

Outline

The Power of Recursive Definitions

So far: only finite state spaces

Example 3.1 (Counter)

$$C = up.(C \parallel down.\mathrm{nil})$$

gives rise to infinite LTS (abbreviating $down := down.\mathrm{nil}$):

$$\begin{tikzcd}
{} \arrow[r] & \boxed{C} \arrow[r, "up"] & \boxed{C \parallel down} \arrow[r, "up"] \arrow[d, "down"] & \boxed{C \parallel down \parallel down} \arrow[r, "up"] \arrow[d, "down"] & \boxed{\cdots} \\
 & & \boxed{C \parallel \mathrm{nil}} \arrow[r, "up"] & \boxed{C \parallel down \parallel \mathrm{nil}} \arrow[r, "up"] \arrow[d, "down"] & \boxed{\cdots} \\
 & & & \boxed{C \parallel \mathrm{nil} \parallel \mathrm{nil}} \arrow[r, "up"] & \boxed{\cdots}
\end{tikzcd}$$

Sequential "specification": $C_0 = up.C_1$
$C_n = up.C_{n+1} + down.C_{n-1} \qquad (n > 0)$

Outline

Process Traces I

Goal: reduce processes to the action sequences they can perform

Definition 3.2 (Trace language)

For every $P \in Prc$, let

$$Tr(P) := \{w \in Act^* \mid \text{ex. } P' \in Prc \text{ such that } P \xrightarrow{w} P'\}$$

be the trace language of P
(where $\xrightarrow{w} := \xrightarrow{a_1} \circ \ldots \circ \xrightarrow{a_n}$ for $w = a_1 \ldots a_n$).

$P, Q \in Prc$ are called trace equivalent if $Tr(P) = Tr(Q)$.

Example 3.3 (One-place buffer)

$B = in.\overline{out}.B$

$\implies \; Tr(B) = (in \cdot \overline{out})^* \cdot (in + \varepsilon)$

Process Traces II

Remarks:

- The trace language of $P \in Prc$ is accepted by the LTS of P, interpreted as a (finite or infinite) automaton with initial state P and where every state is final.
- Trace equivalence is obviously an equivalence relation (i.e., reflexive, symmetric, and transitive).
- Trace equivalence identifies processes with identical LTSs: the trace language of a process consists of the (finite) paths in the LTS. Thus:
$$LTS(P) = LTS(Q) \implies Tr(P) = Tr(Q)$$
- Later we will see: trace equivalence is too coarse, i.e., identifies too many processes
$\implies$ bisimulation

Outline

Motivation

Goal: check processes for simple properties

- action a is initially enabled
- action b is initially disabled
- a deadlock never occurs
- always sends a reply after receiving a request

- formalisation in Hennessy-Milner Logic (HML)
- M. Hennessy, R. Milner: *On Observing Nondeterminism and Concurrency*, ICALP 1980, Springer LNCS 85, 299–309
- checking by exploration of state space

Syntax of HML

Definition 3.4 (Syntax of HML)

The set *HMF* of Hennessy-Milner formulae over a set of actions *Act* is defined by the following syntax:

$$\begin{array}{rcll} F & ::= & \mathrm{tt} & \text{(true)} \\ & \mid & \mathrm{ff} & \text{(false)} \\ & \mid & F_1 \wedge F_2 & \text{(conjunction)} \\ & \mid & F_1 \vee F_2 & \text{(disjunction)} \\ & \mid & \langle\alpha\rangle F & \text{(diamond)} \\ & \mid & [\alpha] F & \text{(box)} \end{array}$$

where $\alpha \in Act$.

Abbreviations for $L = \{\alpha_1, \ldots, \alpha_n\}$ ($n \in \mathbb{N}$):

- $\langle L\rangle F := \langle\alpha_1\rangle F \vee \ldots \vee \langle\alpha_n\rangle F$
- $[L]F := [\alpha_1]F \wedge \ldots \wedge [\alpha_n]F$
- In particular, $\langle\emptyset\rangle F := \mathrm{ff}$ and $[\emptyset]F := \mathrm{tt}$

Meaning of HML Constructs

- All processes satisfy tt.
- No process satisfies ff.
- A process satisfies $F \wedge G$ iff it satisfies F and G.
- A process satisfies $F \vee G$ iff it satisfies either F or G or both.
- A process satisfies $\langle\alpha\rangle F$ for some $\alpha \in Act$ iff it affords an α-labelled transition to a state satisfying F (possibility).
- A process satisfies $[\alpha]F$ for some $\alpha \in Act$ iff all its α-labelled transitions lead to a state satisfying F (necessity).

Semantics of HML

Definition 3.5 (Semantics of HML)

Let $(S, Act, \longrightarrow)$ be an LTS and $F \in HMF$. The set of processes in S that satisfy F, $[\![F]\!] \subseteq S$, is defined by

$$\begin{aligned}
[\![\mathrm{tt}]\!] &:= S & [\![\mathrm{ff}]\!] &:= \emptyset \\
[\![F_1 \wedge F_2]\!] &:= [\![F_1]\!] \cap [\![F_2]\!] & [\![F_1 \vee F_2]\!] &:= [\![F_1]\!] \cup [\![F_2]\!] \\
[\![\langle\alpha\rangle F]\!] &:= \langle\cdot\alpha\cdot\rangle([\![F]\!]) & [\![[\alpha]F]\!] &:= [\cdot\alpha\cdot]([\![F]\!])
\end{aligned}$$

where $\langle\cdot\alpha\cdot\rangle, [\cdot\alpha\cdot] : 2^S \to 2^S$ are given by

$$\begin{aligned}
\langle\cdot\alpha\cdot\rangle(T) &:= \{s \in S \mid \exists s' \in T : s \xrightarrow{\alpha} s'\} \\
[\cdot\alpha\cdot](T) &:= \{s \in S \mid \forall s' \in S : s \xrightarrow{\alpha} s' \implies s' \in T\}
\end{aligned}$$

We write $s \models F$ iff $s \in [\![F]\!]$. Two HML formulae are equivalent (written $F \equiv G$) iff they are satisfied by the same processes in every LTS.

Example 3.6 ($\langle\cdot\alpha\cdot\rangle, [\cdot\alpha\cdot]$ operators)

on the board

Simple Properties Revisited

Example 3.7

1. action a is initially enabled: $\langle a\rangle \mathrm{tt}$
$$\begin{aligned}[\![\langle a\rangle \mathrm{tt}]\!] &= \langle\cdot a\cdot\rangle[\![\mathrm{tt}]\!] = \langle\cdot a\cdot\rangle(S)\\ &= \{s \in S \mid \exists s' \in S : s \xrightarrow{a} s'\} =: \{s \in S \mid s \xrightarrow{a}\}\end{aligned}$$
2. action b is initially disabled: $[b]\mathrm{ff}$
$$\begin{aligned}[\![[b]\mathrm{ff}]\!] &= [\cdot b\cdot][\![\mathrm{ff}]\!] = [\cdot b\cdot](\emptyset)\\ &= \{s \in S \mid \forall s' \in S : s \xrightarrow{b} s' \implies s' \in \emptyset\}\\ &= \{s \in S \mid \nexists s' \in S : s \xrightarrow{b} s'\} =: \{s \in S \mid s \not\xrightarrow{b}\}\end{aligned}$$
3. absence of deadlock:
   - initially: $\langle Act\rangle \mathrm{tt}$
   - always: later (requires recursion)
4. responsiveness:
   - initially: $[request]\langle\overline{reply}\rangle \mathrm{tt}$
   - always: later (requires recursion)

Outline

Closure under Negation

Observation: negation is *not* one of the HML constructs
Reason: HML is closed under negation

Lemma 3.8

For every $F \in HMF$ there exists $F^c \in HMF$ such that $[\![F^c]\!] = S \setminus [\![F]\!]$ for every LTS $(S, Act, \longrightarrow)$.

Proof.

Definition of F^c:

$$\begin{aligned} \mathrm{tt}^c &:= \mathrm{ff} & \qquad \mathrm{ff}^c &:= \mathrm{tt} \\ (F_1 \wedge F_2)^c &:= F_1^c \vee F_2^c & \qquad (F_1 \vee F_2)^c &:= F_1^c \wedge F_2^c \\ (\langle\alpha\rangle F)^c &:= [\alpha]F^c & \qquad ([\alpha]F)^c &:= \langle\alpha\rangle F^c \end{aligned}$$

$[\![F^c]\!] = S \setminus [\![F]\!]$: on the board □