



CCS: Property Specification

Reading: Slides

Mads Dam

Temporal Logics for CCS

Goal: Logic to express interesting correctness properties for CCS

CCS:

Standard labelled transition system so LTL and CTL applies

Here:

Introduce very powerful temporal logic – mu-calculus
Strong ties to bisimulation equivalence

Modal Logic

Logic for possibility/contingency and necessity

$\langle \rangle \phi$: ϕ is possible

$[\] \phi$: ϕ is necessary

Kripke structure: Possible worlds and accessibility relation

$w : \langle \rangle \phi$: ϕ holds in some w' accessible from w

$w : [\] \phi$: ϕ holds in all w' accessible from w

Here: Use a labelled accessibility relation \rightarrow^α

Note:

LTL and CTL are themselves modal logics, with modalities such as O, AX, EX, F, G, U (binary), AF, etc.

Hennessy-Milner Logic - HML

Modal logic with labelled accessibility/transition relation

$P \models \langle \alpha \rangle \phi$ ϕ holds in some P' such that $P \rightarrow^\alpha P'$

$P \models [\alpha] \phi$ ϕ holds in all P' such that $P \rightarrow^\alpha P'$

Directly representable as unary FOL predicate:

$(\langle \alpha \rangle \phi)(P)$ iff $\exists P'. P \rightarrow^\alpha P' \wedge \phi(P')$

$([\alpha] \phi)(P)$ iff $\forall P'. P \rightarrow^\alpha P' \text{ implies } \phi(P')$

HML syntax:

$\phi ::= \text{true} \mid \text{false} \mid \phi \vee \psi \mid \phi \wedge \psi \mid \langle \alpha \rangle \phi \mid [\alpha] \phi$

Positive form, no negation needed

De Morgan: $\neg \langle \alpha \rangle \phi = [\alpha] \neg \phi$, $\neg [\alpha] \phi = \langle \alpha \rangle \neg \phi$

HML - Examples

- $P \models \langle \text{in} \rangle \text{true}$ an "in" action is possible in state P
- $P \models [\text{out}] \text{false}$ no "out" action is possible in state P
- $P \models \langle \text{in} \rangle \langle \text{out} \rangle \text{true}$...
- $P \models \langle \text{in} \rangle [\text{in}] \text{false}$...

Distinguishing formula:

$\langle a \rangle [b] \text{false}$ distinguishes $a.b.0 + a.c.0$ from $a.(b.0 + c.0)$

HML *characterises* strong bisimulation equivalence for CCS:

Theorem (Modal Characterisation): Provided all process definitions are guarded, the following statements are equivalent for P, Q guarded:

1. $P \sim Q$
2. For all HML formulas ϕ , if $P \models \phi$ then $Q \models \phi$

Proof of Modal Characterisation

(This material is intermediate level)

1 \rightarrow 2: Use induction on structure of ϕ

2 \rightarrow 1: Let:

$P \sim_0 Q$ (always)

$P \sim_{i+1} Q$ iff

- whenever $P \rightarrow^\alpha P'$ then exists Q' such that $Q \rightarrow^\alpha Q'$ and $P' \sim_i Q'$
- whenever $Q \rightarrow^\alpha Q'$ then exists P' such that $P \rightarrow^\alpha P'$ and $P' \sim_i Q'$

Exercise: Show that for all $i \in \mathbb{N}$, $\sim_i \supseteq \sim_{i+1}$ (monotonicity)

Let $P \sim' Q$ iff $P \sim_i Q$ for all $i \in \mathbb{N}$

Exercise: Show that $P \sim' Q$ if $P \sim Q$

Exercise: Show that if P is guarded then $\{P' \mid P \rightarrow^\alpha P'\}$ is finite (terminology: P is image finite)

Modal Characterisation, II

We show $P \sim' Q$ implies $P \sim Q$.

If $P \rightarrow^\alpha P'$ then there exists some Q' such that for infinitely many $i \in \mathbb{N}$,
 $Q \rightarrow^\alpha Q'$ and $P' \sim_i Q'$

This follows from image finiteness

But then $P' \sim_i Q'$ for all $i \in \mathbb{N}$

This follows from monotonicity

Symmetrically, if $Q \rightarrow^\alpha Q'$ some P' can be found

But then \sim' is a strong bisimulation relation, so $P \sim Q$

So if $P \approx Q$ then there is some $i \in \mathbb{N}$ such that $P \approx_i Q$

Use this to construct HML formula $\phi_{P,i}$ such that $P \models \phi$ and $Q \not\models \neg\phi$

Modal Characterisation, III

Suppose $P \approx_i Q$

Construct $\phi_{P,i}$ by induction on i

Base case, $i = 0$: Immediate contradiction since $P \sim_0 Q$

Induction step, $i = i'+1$:

Let $\phi_{P,i} = \bigwedge \{ \langle \alpha \rangle \phi_{P',i'} \mid P \rightarrow^\alpha P' \} \wedge (\bigwedge_\alpha [\alpha] (\bigvee \{ \phi_{P',i'} \mid P \rightarrow^\alpha P' \}))$

Use induction to show $P \models \phi_{P,i}$

Since $P \approx_i Q$ either

- $P \rightarrow^\alpha P'$, some P' , and whenever $Q \rightarrow^\alpha Q'$ then $P' \approx_{i'} Q'$, or
- $Q \rightarrow^\alpha Q'$, some Q' , and whenever $P \rightarrow^\alpha P'$ then $P' \approx_{i'} Q'$

In either case the argument is closed by the induction hypothesis

Exercise: Fill in the details

A Proof System for HML

$$\mathbf{True} \frac{-}{P : \text{true}}$$

$$\mathbf{Or}_L \frac{P : \varphi}{P : \varphi \vee \psi}$$

$$\mathbf{Or}_R \frac{P : \varphi}{P : \psi \vee \varphi}$$

$$\mathbf{And} \frac{P : \varphi \quad P : \psi}{P : \varphi \wedge \psi}$$

$$\mathbf{Dia} \frac{P' : \varphi}{P : \langle \alpha \rangle \varphi} (P \rightarrow^\alpha P')$$

$$\mathbf{Box} \frac{P_1 : \varphi \quad \dots \quad P_n : \varphi}{P : [\alpha] \varphi} (\{P_1, \dots, P_n\} = \{P' \mid P \rightarrow^\alpha P'\})$$

Extensions

Action sets

- Sets $L \subseteq \text{Act}$ label the modalities $\langle L \rangle \varphi$, $[L] \varphi$
- $\rightarrow^\dagger = \cup \{ \rightarrow^\alpha \mid \alpha \in L \}$
- Complementation:
 - L abbreviates $\text{Act} - L$
 - \emptyset abbreviates $\text{Act} - \emptyset$
- Examples: $[-] \text{false}$, $[\text{in}][-\text{out}] \text{false}$

Weak modalities $\langle \langle L \rangle \rangle$, $[[L]]$:

- Refer to the weak transition relations
- Example: $[[\text{in}]] [[-\text{out}, \text{eps}]] \text{false}$

Adding Recursion to HML

Adding a temporal dimension to HML

Observation: CTL operators are recursive, e.g. $AG\phi = \phi \wedge AXAG\phi$

Unfortunately, equations do not have unique solutions

Which sets satisfy the equation $X = \langle \alpha \rangle X$?

- Sol'n 1: $X = \text{false}$
- Sol'n 2: $X = \varphi = \{P_0 \mid \text{for all } i > 0 \text{ there is } P_i \text{ such that } P_{i-1} \rightarrow^\alpha P_i\}$

Sol'n 1: least solution, $\mu X. \langle \alpha \rangle X$

Sol'n 2: greatest solution, $\nu X. \langle \alpha \rangle X$

μ - Calculus, II

Unfolding fixed point formulas (σ is either μ or ν):

$$\sigma X. \varphi = \varphi[\sigma X. \varphi / X]$$

$$\text{Example: } \nu X. \langle \alpha \rangle X = \langle \alpha \rangle \nu X. \langle \alpha \rangle X = \langle \alpha \rangle \langle \alpha \rangle \nu X. \langle \alpha \rangle X \dots$$

Fixed point approximants:

$$\mu^0 X. \varphi = \text{false}$$

$$\nu^0 X. \varphi = \text{true}$$

$$\mu^{k+1} X. \varphi = \varphi[\mu^k X. \varphi / X]$$

$$\nu^{k+1} X. \varphi = \varphi[\nu^k X. \varphi / X]$$

Knaster-Tarski Theorem (for CCS and strong transitions):

$$\mu X. \varphi = \exists k. \mu^k X. \varphi$$

$$\nu X. \varphi = \forall k. \nu^k X. \varphi$$

Note that:

$$\mu^0 X. \varphi \subseteq \mu^1 X. \varphi \subseteq \mu^2 X. \varphi \subseteq \dots \subseteq \mu X. \varphi$$

$$\nu^0 X. \varphi \supseteq \nu^1 X. \varphi \supseteq \nu^2 X. \varphi \supseteq \dots \supseteq \nu X. \varphi$$

Example Properties

μ -calculus: Tiny programming language for program properties

AG ϕ	$\forall X. \phi \wedge [-]X$
terminates	$\mu X. [-]X$
AF ϕ	$\mu X. \phi \vee (\langle\langle\rightarrow\text{tt}\rangle\rangle \wedge [-]X)$
$A(\phi \cup \psi)$	$\mu X. \psi \vee (\phi \wedge [-]X)$
Eventually α has to be taken	$\mu X. \langle\langle\rightarrow\text{tt}\rangle\rangle \wedge [-\alpha]X$
On all paths infinitely often ϕ	$\forall X. \mu Y. (\phi \wedge [-] X) \vee [-]Y$
$\langle\langle\rightarrow\rightarrow\rangle\rangle \phi$	$\mu X. \phi \vee \langle\langle\tau\rangle\rangle X$
$\langle\langle\alpha\rangle\rangle \phi$	$\langle\langle\rightarrow\rightarrow\rangle\rangle \langle\langle\alpha\rangle\rangle \langle\langle\rightarrow\rightarrow\rangle\rangle \phi$

Point to note: Once some abbreviation has been introduced it's free to be used, of course.

Example: Buffer Properties

Ongoing capability	$\forall X. \langle\langle\text{in}\rangle\rangle \langle\langle\overline{\text{out}}\rangle\rangle X$
Alternation of in and out	AG $[[\text{in}]] [[\overline{\text{out}}]] \text{false}$ AG $[[\overline{\text{out}}]] [[\text{in}]] \text{false}$
Deadlock freedom	AG $\langle\langle\rightarrow\text{tt}\rangle\rangle$
Progress	AG $\mu X. [\tau]X$

Word of warning: It's easy to say "alternation of in and out". What do you actually mean?

More precisely: Which property of infinite labelled trees are you after?

Proof Rules for Fixed Point Formulas

Let A be a set of CCS terms:

$P \models \nu^A X. \varphi$ means $P \models \varphi[\nu^{A \cup \{P\}} X. \varphi / X]$ or $P \in A$

$P \models \mu^A X. \varphi$ means $P \models \varphi[\mu^{A \cup \{P\}} X. \varphi / X]$ and $P \notin A$

Idea: Has P been already visited?

Proof rules:

$$\mathbf{Fix}_1 \frac{P : \varphi[\sigma^{A,P} X. \varphi / X]}{P : \sigma^A X. \varphi} (P \notin A) \quad \mathbf{Fix}_2 \frac{-}{P : \nu^A X. \varphi} (P \in A)$$

And a "negative" rule:

$$\mathbf{Fix}_3 \frac{P : \mu^A X. \varphi}{- \text{give up} -} (P \in A)$$

Example

$\text{Buf} = \text{in.out.Buf}$

$\text{Sys} = (\text{Buf}[\overline{\text{comm}}/\text{out}] \mid \text{Buf}[\text{comm}/\text{in}]) \setminus \{\text{comm}\}$

$\text{Spec} = \text{"On all paths infinitely often out is possible"}$

$= \nu X. \mu Y. (\langle \text{out} \rangle \text{true} \wedge [-]X) \vee [-]Y$

Prove $\text{Sys} : \text{Spec}$

Proof given in class