Maximal Traces and Path-Based Coalgebraic Temporal Logics

Corina Cîrstea

Electronics and Computer Science
University of Southampton

Overview

- logics for bisimulation well understood in a coalgebraic setting
- no coalgebraic semantics for path-based temporal specification logics:
  - CTL* on transition systems
  - PCTL on probabilistic transition systems

This talk:

- maximal traces and computation paths
  - existing general theory of *finite* traces [Hasuo et. al.]
  - existing definition of *infinite* traces for $T = \mathcal{P}$ [Jacobs '04]
- coalgebraic semantics for path-based temporal logics

Finite Traces, Coalgebraically

[Hasuo et. al.] consider $T \circ F$-coalgebras, where:

- strong monad $T : \mathsf{C} \to \mathsf{C}$ describes the computation/branching type

  e.g. $\mathcal{P}$, $\mathcal{S}$

- functor $F : \mathsf{C} \to \mathsf{C}$ describes the transition type
  - initial F-algebra gives possibile *finite* traces

  e.g. Id, $A \times \mathsf{Id}$, $1 + A \times \mathsf{Id}$

- distributive law $\lambda : F \circ T \Rightarrow T \circ F$ as parameter

Restricted Transition Systems and CTL*

- restricted transition systems are $\mathcal{P}^+$-coalgebras
- to each state, one associates a set of computation paths

CTL*:

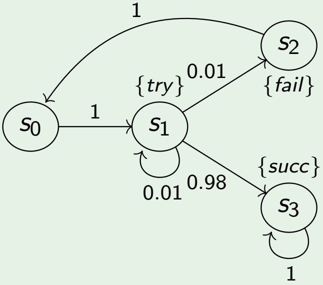
- path formulas: $\varphi ::= \phi \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathbf{X}\varphi \mid \mathbf{F}\varphi \mid \mathbf{G}\varphi \mid \varphi\mathbf{U}\varphi$
- state formulas: $\phi ::= \mathrm{tt} \mid p \mid \neg\phi \mid \phi \wedge \phi \mid \mathbf{E}\varphi \mid \mathbf{A}\varphi$
  - **E** and **A** similar to $\Diamond$ and $\Box$ modalities ...

Probabilistic Transition Systems

- probabilistic transition systems are $\mathcal{D}$-coalgebras

  ($\mathcal{D}(S)$ = set of probability distributions over S)

Example



Some computation paths from s_0:

$s_0 \to s_1 \to s_1 \ldots$

$s_0 \to s_1 \to s_2 \to s_0 \to s_1 \to s_2 \ldots$

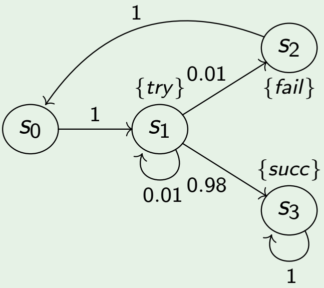
$s_0 \to s_1 \to s_3 \to s_3 \ldots$

- to each state, one associates a probability measure on the computation paths from that state

The Logic PCTL

- path formulas: $\varphi ::= \mathbf{X}\phi \mid \phi \mathbf{U}^{\leq t}\phi \qquad t \in \{0, 1, \ldots\} \cup \{\infty\}$
- state formulas: $\phi ::= \mathrm{tt} \mid p \mid \neg\phi \mid \phi \wedge \phi \mid [\varphi]_{\geq q} \mid [\varphi]_{>q}$

Example



$[\mathrm{tt}\mathbf{U}^{\leq 3} \mathit{fail}]_{<0.1}$

$[(\mathit{try}\,\mathbf{U}\,\mathit{succ})]_{\geq 1}$

More Examples

- (restricted) labelled transition systems (LTSs) are $\mathcal{P}^+(A \times \mathsf{Id})$-coalgebras
- generative probabilistic transition systems (GPTSs) are $\mathcal{D}(A \times \mathsf{Id})$-coalgebras

For *both* LTSs and GPTSs, computation paths have the form

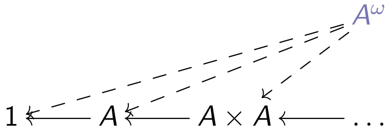
$$s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} s_2 \xrightarrow{a_2} \dots$$

whereas infinite computation traces have the form

$$a_0\, a_1\, a_2 \dots$$

Towards Maximal Traces

- the possible infinite traces for both LTSs and GPTSs are elements of A^ω (the *final* $A \times \_$-coalgebra):



- for an LTS/GPTS (S, γ), the actual maximal traces should be *structured* according to the computation type:

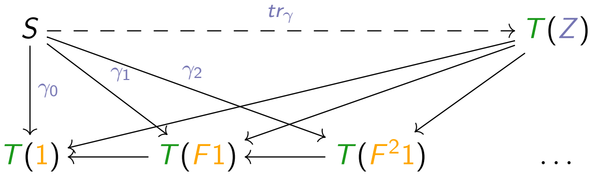
$$tr_\gamma : S \to \mathcal{P}^+(A^\omega) \quad \text{or} \quad tr_\gamma : S \to \mathcal{D}(A^\omega)$$

- in general, the maximal trace map should have the form:

$$tr_\gamma : S \to T(Z)$$

Defining the Maximal Trace Map

Fix a $T \circ F$-coalgebra $\gamma : S \to TFS$.

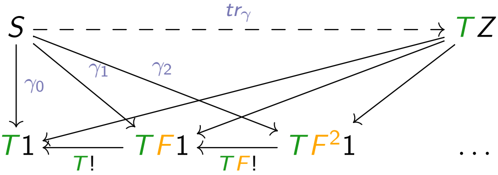


Define $tr_\gamma : S \to T(Z)$ from its finite approximants γ_i.

For existence of tr_γ, we need:

- γ_i's define a cone (true for *affine* monads)
- limiting property for $T(Z)$

Defining the γ_is

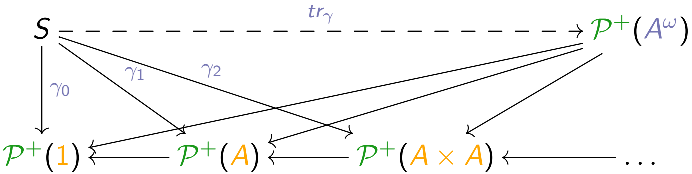


γ_0: $$S \xrightarrow{!_S} 1 \xrightarrow{\eta_1} T1$$

γ_{i+1}: $$S \xrightarrow{\gamma} TFS \xrightarrow{TF\gamma_i} TFTF^i 1 \xrightarrow{T\lambda_{F^i 1}} T^2 F^{i+1} 1 \xrightarrow{\mu_{F^{i+1} 1}} TF^{i+1} 1$$

For T *affine*, the γ_is define a cone (also in Kl(T)).

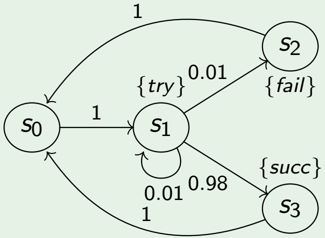
The Case of Non-deterministic Systems



- for $T = \mathcal{P}^+$, cone is only *weakly* limiting
  - $\Rightarrow$ take *maximal* mediating map !

The Case of Probabilistic Systems

Example



- working with $T = \mathcal{D}$ over sets does not work:
  - probability measures needed to deal with *uncountably many* traces

$\Rightarrow$ need to work with $T = \mathcal{G}$ over (standard Borel) measurable spaces

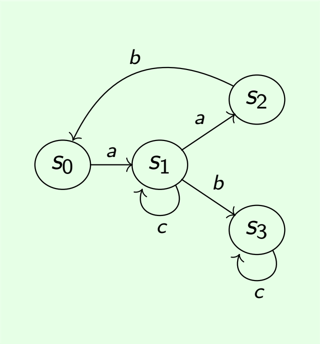
- resulting maximal trace map takes states to probability measures over maximal traces

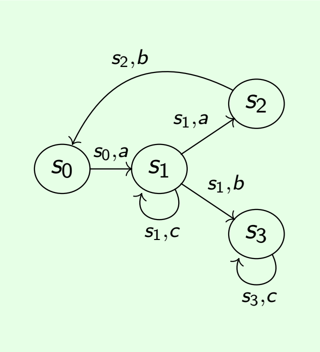
The Case of Probabilistic Systems (Cont'd)

1. start with a $\mathcal{D} \circ F$-coalgebra γ over Set
2. lift $F : \mathsf{Set} \to \mathsf{Set}$ to $\tilde{F} : \mathsf{Meas} \to \mathsf{Meas}$ (works for *certain polynomial* F*s*)
3. obtain a $\mathcal{G} \circ \tilde{F}$-coalgebra $\tilde{\gamma}$ over Meas, to which the definition can be applied:
    - we obtain a cone (for any F as above)
    - $\mathcal{G} : \mathsf{Meas} \to \mathsf{Meas}$ preserves the required limit

From Maximal Traces to Maximal Executions

- view $\mathcal{P}^+(A \times \_)$-coalgebra: as $\mathcal{P}^+(S \times A \times \_)$:





- obtain a maximal execution map $exec_\gamma : S \to (S \times A)^\omega$ as the maximal trace map of the new coalgebra !!

Maximal Executions: Examples

Take $T = \mathcal{P}^+$.

- $F = \_$ (restricted TSs):

$$s_0\ s_1\ s_2\ \ldots$$

- $F = A \times \_$ (restricted LTSs):

$$s_0\ a_1\ s_1\ a_2\ s_2\ \ldots$$

- $F = 1 + A \times \_$ (LTSs):

$$s_0\ a_1\ s_1\ a_2\ s_2\ \ldots \qquad \text{or} \qquad s_0\ a_1\ s_1\ \ldots\ s_n$$

Towards Path-Based Temporal Logics

$T \circ F$-coalgebra (X, γ) comes with execution map $exec_\gamma : X \to T(Z_X)$

$\Longrightarrow$ use modalities for T to "quantify" over maximal executions

$X \times F\_$-coalgebra structure on maximal executions Z_X gives, for each execution:

- the first state,
- an F-structured successor.

$\Longrightarrow$ use modalities for F to talk about maximal executions

From Coalgebraic Types to Path-Based Temporal Logics

- coalgebraic types come equipped with modal languages
  - $T = \mathcal{P}^+$: modal operators $\Box$ and $\Diamond$:

    $s \models \Box\phi$ iff $s' \models \phi$ for all s' s.t. $s \to s'$

    $s \models \Diamond\phi$ iff $s' \models \phi$ for some s' s.t. $s \to s'$

  - $T = \mathcal{D}$: modal operator L_p

    $s \models L_p\phi$ iff $\gamma(s)(\llbracket\phi\rrbracket) \geq p$

  - $F = A \times \_$: modal operators a and $\mathbf{X}$:

    $s \models a$ iff $s \to (a, s')$

    $s \models \mathbf{X}\phi$ iff $s \to (a, s')$ and $s' \models \phi$

- our coalgebras have type $T \circ F$ ...

Path-Based Temporal Logics in a Nutshell

- maximal executions form an $X \times F$-coalgebra $Z_X \to X \times FZ_X$

  $\Longrightarrow$ use fixpoint logics for F-coalgebras to define path formulas:

  - $\varphi ::= \mathsf{tt} \mid \mathsf{ff} \mid p^F \mid \phi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid [\lambda_F]\varphi \mid \mu p^F.\varphi \mid \nu p^F.\varphi$
  - standard definition for $(\!|\varphi|\!) \in P(Z_X)$

- use non-standard interpretation of modal operators for T:

  $\phi ::= \mathsf{tt} \mid \mathsf{ff} \mid p \mid \phi \wedge \phi \mid \phi \vee \phi \mid [\lambda_T]\varphi$

  - $X \xrightarrow{\mathsf{exec}_\gamma} TZ_X$

$$[\![\phi]\!] \in P(X) \xleftarrow{P(\mathsf{exec}_\gamma)} P(TZ_X) \xleftarrow{(\lambda_T)_Z} P(Z_X) \ni (\!|\phi|\!)$$

LCTL*

$T = \mathcal{P}^+$ with modal operators $\Box, \Diamond$

$F = A \times \mathsf{Id}$ with modal operators a ($a \in A$), $\mathbf{X}$

$$\Longrightarrow \quad \varphi \;::=\; \mathsf{tt} \mid \mathsf{ff} \mid p^F \mid \phi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid a \mid \mathbf{X}\varphi \mid \mu p^F.\varphi \mid \nu p^F.\varphi$$

$$\phi \;::=\; \mathsf{tt} \mid \mathsf{ff} \mid p \mid \phi \wedge \phi \mid \phi \vee \phi \mid \Box\varphi \mid \Diamond\varphi$$

- can refer to the *next label along a path*:
  - natural encoding of "a occurs along every path" as

    $$\Box\, F a \;::=\; \Box\, \mu X.(\, a \vee \mathbf{X} X\,)$$

  - compare above to

    $$\mu X.(\, \langle \_ \rangle \mathsf{tt} \wedge [-a] X\,)$$

PCTL Coalgebraically

$T = \mathcal{D}$ with modal operator L_q

$F = \mathsf{Id}$ with modal operator $\mathbf{X}$

$$\Longrightarrow \quad \varphi ::= \mathsf{tt} \mid \mathsf{ff} \mid p^F \mid \phi \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathbf{X}\varphi \mid \mu p^F.\varphi \mid \nu p^F.\varphi$$

$$\phi ::= \mathsf{tt} \mid p \mid \neg\phi \mid \phi \wedge \phi \mid L_q\varphi$$

Define:

- $\mathbf{X}\varphi ::= \mathbf{X}\varphi$
- $\varphi \mathbf{U}^\infty \psi ::= \mu X.(\psi \vee (\phi \wedge \mathbf{X}X))$
- $[\varphi]_{\geq q} ::= L_q\varphi$

Can also obtain version of PCTL on generative PTSs . . .

Some Results

- for $\mathcal{P}^+ \circ F$-coalgebras (F polynomial), traces are characterised by an F-coalgebra automaton

  $\Longrightarrow$ regular game for model-checking *linear* path-based logics

  [CALCO 2011]

- *linear* path-based logics sufficient to characterise traces

Future Work

- other (non-affine) computational monads
  - e.g. the finite multiset monad and graded temporal logics
- automata-based coalgebraic model checking