Intentional Labeled Transition Systems

Sophie Pinchinat
IRISA-INRIA
Campus de Beaulieu
F-35042, Rennes - France
Sophie.Pinchinat@irisa.fr

Plan

- Intentionally-Labeled Transition Systems
  - Relation with LTS
  - Combining Systems
  - Notion of Bisimulation
- Intentional Labeled Transition Systems
  - Parallel Composition
  - Bisimulation
- Symbolic Systems
- A Multi-Agents Framework
- Concluding Remarks (The Tool SIGALI)

First order language : syntax

- $\mathcal{L}$ a first order language

  Connectors $\wedge$, $\neg$, and the derived symbols $\vee$, $\Rightarrow$, $\Leftrightarrow$

  Quantifiers $\forall$, $\exists$

  Variables symbols an infinite set $E = \{e, e', ...\}$

  Predicate symbols $\rho, \rho_1, ...$

  Function symbols $f, g, ...$

Formulas $\mathcal{F}(\mathcal{L}) = \{F, F_1, ...\}$

- $F(e_1, e_2, ..., e_m)$ means e_i is free in F
- Given $\mathcal{F}_1$ and $\mathcal{F}_2$ two sets of formulas

  $\mathcal{F}_1 \wedge \mathcal{F}_2$ is $\{F_1 \wedge F_2 | F_i \in \mathcal{F}_i\}$
- Given $E' = \{e_1, ..., e_m\} \subseteq E$

  $\exists E'.F$ is $\exists e_1 \exists e_2 ... \exists e_m F$

First order language : semantics

- Interpretation $\mathcal{D}$

  Domain of values D

  Meaning of the symbols $f^{\mathcal{D}}, P^{\mathcal{D}}, \ldots$ and valuation of variables

- $(d_1, d_2, \ldots, d_m) \approx^{\mathcal{D}} F(e_1, e_2, \ldots, e_m)$ means
  the interpretation of F on $\mathcal{D}$ with valuation $e_i \mapsto d_i$, $\forall i$ is true.

- $F^{\mathcal{D}}(e_1, e_2, \ldots, e_m)[d/e_i]$ for $d \in \mathcal{D}$
  the $(d_1, \ldots, d_{i-1}, d_{i+1}, \ldots, d_m) \in D^{m-1}$ s.t.
  $(d_1, \ldots, d_{i-1}, d, d_{i+1}, \ldots, d_m) \approx^{\mathcal{D}} F(e_1, e_2, \ldots, e_m)$.

- $\approx^{\mathcal{D}} F(e_1, e_2, \ldots, e_m)$ means
  $(d_1, d_2, \ldots, d_m) \approx^{\mathcal{D}} F(e_1, e_2, \ldots, e_m)$, for all $(d_1, d_2, \ldots, d_m) \in D^m$

Notations

- `true` is any tautology
- $F[t/e]$ is the formula F in which any free occurrence of the variable e is replaced by t, a term of $\mathcal{L}$.
- Given $F(e_1, ..., e_m) \in \mathcal{F}(\mathcal{L})$ and an interpretation $\mathcal{D}$

  $Sol_{\mathcal{D}}(F)$ is the set of $(d_1, ..., d_m) \in D^m$ s.t. $(d_1, ..., d_m) \models\!\!\approx F(d_1, ..., d_m)$.
- $\mathcal{L}$ and $E = \{e_1, e_2, ..., e_m\}$

  $\mathcal{F}_E(\mathcal{L})$ the set of formulas of $\mathcal{L}$ which free variables range over E

Intentionally-Labeled Transition Systems

- $\mathsf{S} = (S, \mathcal{F}_E(\mathcal{L}), T, I)$ is a classic Transition System labeled on $\mathcal{F}_E(\mathcal{L})$

$$s \stackrel{F}{\to} s'$$

S states ; $I \subseteq S$ are the initial states

$T : S \times \mathcal{F}_E(\mathcal{L}) \times S$ is the transition relation

Transitions are $\underbrace{\text{labeled by formulas}}_{\text{intentionally-labeled}}$ in $\mathcal{F}_E(\mathcal{L})$

- E the set of event variables and $Car(E)$ is the dimension of S

From iLTS to LTS

- Let $\mathtt{S} = (S, \mathcal{F}, T, I)$ be an iLTS of dimension m on $(\mathcal{L}, E)$
- Each interpretation $\mathcal{D}$ for the formulas delivers an (exhaustive) labeled transition system over D^m written $\mathtt{LTS}(\mathtt{S}, \mathcal{D}) = (S, D^m, T, I)$

$$s \stackrel{(d_1,\ldots,d_m)}{\longrightarrow} s' \text{ whenever } \begin{cases} s \stackrel{F}{\rightarrow} s' \text{ and} \\ (d_1, \ldots, d_m) \in Sol_{\mathcal{D}}(F(e_1, \ldots, e_m)) \end{cases}$$

- $\mathtt{LTS}(\mathtt{S}, \mathcal{D})$ is finite if S, $\mathcal{F}$, and $\mathcal{D}$ are finite

From LTS to iLTS

- From the LTS $\mathcal{S}$ (on domain D), build $\mathtt{iLTS}(\mathcal{S})$ of dimension 1.

$$s \xrightarrow{d} s' \qquad \text{becomes} \qquad s \xrightarrow{e=f_d} s'$$

- $\mathtt{iLTS}(\mathcal{S})$ relies on the first order language where

  $E = \{e\}$ is a singleton set of variables

  f_d a function symbol for each $d \in D$ of arity 0 ; a constant

  $=$ the equality predicate

Theorem For the interpretation $\mathcal{D}$ where f_d^D is d itself,
the LTS $\mathcal{S}$ and $\mathtt{LTS}(\mathtt{iLTS}(\mathcal{S}), \mathcal{D})$ are bisimilar

iLTS Synchronized Parallel Composition

- $\mathcal{L}$ is fixed, E_1 and E_2 are event variables (think of channels)
- Given $\mathcal{S}_1 = (S_1, \mathcal{F}_1, T_1, I_1)$ of dim. m_1 on $(\mathcal{L}, E_1)$

  $\mathcal{S}_2 = (S_2, \mathcal{F}_2, T_2, I_2)$ of dim. m_2 on $(\mathcal{L}, E_2)$
- $\mathcal{S}_1 \mid \mathcal{S}_2 = (S_1 \times S_2, \mathcal{F}_1 \wedge \mathcal{F}_2, T, I_1 \times I_2)$ where

  $(s_1, s_2) \stackrel{F_1 \wedge F_2}{\rightarrow} (s_1', s_2')$ whenever $s_1 \stackrel{F_1}{\rightarrow} s_1'$ and $s_2 \stackrel{F_2}{\rightarrow} s_2'$

  of dimension $m \leq m_1 + m_2$ in general, as events variables car be shared
- Commutativity and Associativity of $\mid$ is clear
- The definition is simple (more than in the exhaustive framework)

Other Parallel Compositions

- Partially Synchronized Parallel Composition

$$(s_1, s_2) \stackrel{F_1 \wedge \neg(\bigvee_{F \in ev(s_2)} F)}{\longrightarrow} (s_1', s_2) \text{ whenever } s_1 \stackrel{F_1}{\rightarrow} s_1'$$

where $ev(s_2) = \{F | \exists s_2', s_2 \stackrel{F}{\rightarrow} s_2'\}$

- Asynchronous Parallel Composition

$$(s_1, s_2) \stackrel{F}{\rightarrow} (s_1', s_2') \text{ whenever } \begin{cases} s_1 \stackrel{F_1}{\rightarrow} s_1' \text{ and } s_2 = s_2' \text{ and } F = F_1, \text{ or} \\ s_1 = s_1' \text{ and } s_2 \stackrel{F_2}{\rightarrow} s_2' \text{ and } F = F_2 \end{cases}$$

Other Combinators

- Events Hiding $(E' \subseteq E)$

  $(\mathsf{S} \setminus E') = (S, \mathcal{F}', T, I)$ on $E \setminus E'$ is s.t.

  $s_1 \stackrel{\exists E' F}{\rightarrow} s_1'$ whenever $s_1 \stackrel{F}{\rightarrow} s_1'$.

- ...

Symbolic Bisimulation

- $\mathcal{S}_1 = (S_1, \mathcal{F}_1, T_1, I_1)$ and $\mathcal{S}_2 = (S_2, \mathcal{F}_2, T_2, I_2)$ over the same $(\mathcal{L}, E)$ and $\mathcal{D}$ be an interpretation of $\mathcal{L}$.
- A *D-symbolic bisimulation* between $\mathcal{S}_1$ and $\mathcal{S}_2$ is $\mathcal{R} \subseteq S_1 \times S_2$

  $s_1 \mathcal{R} s_2$ iff (1) for all $s_1 \stackrel{F}{\rightarrow} s'_1$, there are finitely many $(s_2 \stackrel{F_j}{\rightarrow} s_2^j)_j$ s.t.
  $\models\!\approx^{\mathcal{D}} (F \Rightarrow \bigvee_j F_j)$, and $s'_1 \mathcal{R} s_2^j \quad \forall j$
  (2) and vice versa.

  Theorem There exists a D-symbolic bisimulation between $\mathcal{S}_1$ and $\mathcal{S}_2$ if and only if there exists a bisimulation between $\mathtt{LTS}(\mathcal{S}_1, \mathcal{D})$ and $\mathtt{LTS}(\mathcal{S}_2, \mathcal{D})$.

Intentional Labeled Transition Systems

- $\mathsf{S} = (X, Y, \mathcal{T}, I)$ an Intentional Labeled Transition Systems (ILTS)

  States variables $X = \{x_1, x_2, ..., x_n\}$ (and a copy $X' = \{x'_1, x'_2, ..., x'_n\}$) is a finite set of variable symbols of $\mathcal{L}$.

  Events variables $Y = \{y_1, y_2, ..., y_m\}$ a set of variable symbol of $\mathcal{L}$ disjoint from $X \cup X'$;

  $\mathcal{T}(x_1, .., x_n, y_1, ..., y_m, x'_1, ..., x'_n)$ or simply $\mathcal{T}(X, Y, X')$ is a formula of $\mathcal{L}$ which free variables range over $X \cup Y \cup X'$;

  $I(x_1, ...x_n)$ is a formula of $\mathcal{L}$.

- $(Card(X), Card(Y))$ is the dimension of S

ILTS Parallel Composition

$$\mathrm{S}_1 \mid \mathrm{S}_2 = (X_1 \cup X_2, Y_1 \cup Y_2, \mathcal{T}_1(X_1, Y_1, X_1') \wedge \mathcal{T}_2(X_2, Y_2, X_2'), I_1(X_1) \wedge I_2(X_2))$$

Resource sharing $X_1 \cap X_2 \neq \emptyset$

Events (or comunication channels) sharing $Y_1 \cap Y_2 \neq \emptyset$

ILTS Bisimulation

- Define $R_0(X_1, X_2) = \mathtt{true}$, and

$$R_{k+1}(X_1, X_2) = R_k(X_1, X_2) \wedge$$

$$\wedge \begin{cases} \forall X_1' \forall Y [\mathcal{T}_1(X_1, Y, X_1') \ \Rightarrow \ \exists X_2' \mathcal{T}_2(X_2, Y, X_2') \wedge R_k(X_1', X_2')] \\ \forall X_2' \forall Y [\mathcal{T}_2(X_2, Y, X_2') \ \Rightarrow \ \exists X_1' \mathcal{T}_1(X_1, Y, X_1') \wedge R_k(X_1', X_2')] \end{cases}$$

- If $\mathcal{D}$ is finite, the logical operations are computable and formulas equivalence on $\mathcal{F}(\mathcal{L})$ is decidable , $R_k^{\mathcal{D}}(X_1, X_2)$ eventually stabilizes (modulo formulas equivalence) as $R^{\mathcal{D}}(X_1, X_2)$

  Theorem For all $d_1 \in D$ and $d_2 \in D$, $R^{\mathcal{D}}(d_1, d_2)$ if and only if d_1 and d_2 are bisimilar (in $\mathtt{LTS}(\mathtt{S}_1, \mathcal{D})$ and $\mathtt{LTS}(\mathtt{S}_2, \mathcal{D})$)

Symbolic Transition Systems

- $\mathcal{T}(X, Y, X')$ is an expression "$P(X, Y, X') = 0$"

  where $P(X, Y, X') \in \mathbb{Z}/p\mathbb{Z}[X \cup Y \cup X']$ (the ring of polynomials) with coefficients in the field $\mathbb{Z}/p\mathbb{Z}$ (p prime)

- $\mathcal{L}$ is

  $\{0, 1, 2, ..., p-1, +, *, -, /\}$ (function symbols)

  $\{=\}$ (predicate symbols)

- $sol(P(X, Y, X')) \stackrel{\text{def}}{=}$

$$\left\{ \begin{array}{l} (d^{x_1}, ..., d^{x_n}, d^{y_1}, ..., d^{y_m}, d^{x'_1}, ..., d^{x'_n}) \in \mathbb{Z}/p\mathbb{Z}^{2n+m} \\ \mid P(d^{x_1}, ..., d^{x_n}, d^{y_1}, ..., d^{y_m}, d^{x'_1}, ..., d^{x'_n}) = 0 \end{array} \right\}$$

Hence $Sol_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{T}(X, Y, X')) = sol(P(X, Y, X'))$

Symbolic Combinators and Computation

- $Sol_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{T}_1(X_1, Y_1, X'_1) \diamond \mathcal{T}_2(X_2, Y_2, X'_2)) =$
  $sol(P_1(X_1, Y_1, X'_1) \diamond P_2(X_2, Y_2, X'_2))$

$P_1 \oplus P_2 \stackrel{\text{def}}{=} (P_1^{p-1} + P_2^{p-1})^{p-1}$	for $\wedge$
$P_1 * P_2$	for $\vee$ connector
$1 - P^{p-1}$	for $\neg$ connector
If $z \in \{X \cup Y \cup X'\}$ $\Pi_{d \in \mathbb{Z}/p\mathbb{Z}} P(X, Y, X')[d/z]$	for $\exists z$

- [Dutertre92] Each $P(X \cup Y \cup X')$ has a computable canonical representative modulo $\langle (X \cup Y \cup X')^p - (X \cup Y \cup X') \rangle$

Implementing Polynomials and Tools

- p-Decision Diagrams

  BDD package Tiger CMU in the SMV Tool [McMillan93]; $p = 2$

  TDD package in the SIGALI Tool [Dutertre-Leborgne93];

  $p = 3$ (1 true, -1 false, 0 absent, in SIGNAL language)

- Since $\mathbb{Z}/p\mathbb{Z}$ is finite, the operations on polynomials and 0-test are computable, $R_k^{\mathbb{Z}/p\mathbb{Z}}(X_1, X_2)$ (modulo $\langle (X_1 \cup X_2)^p - (X_1 \cup X_2) \rangle$) eventually stabilizes

- Use the algorithm to compute the greatest symbolic bisimulation

A Multi-Agents Framework

- Close to Alternating Time Transition Systems [AHK98]
- Suppose m agents $\{1, ..., m\}$, each agent "controls" one component in the vector event $Y = \{t_1, y_2, ..., y_m\}$.
- Assume, we want to characterize by $PreGood(X)$ (the set of) states s.t. agents 1 and 2 can cooperate (against the $m-2$ others) to inevitably reach in one step a given set of states $Good(X)$

$$PreGood(X) = \exists\{y_1, y_2\}\forall\{y_3, \ldots, y_m\}\exists X'[\mathcal{T}(X, Y', X') \wedge Good(X')]$$

$$(x_1, \ldots, x_n) \stackrel{(a,b,*,\ldots,*)}{\rightarrow} (x_1, \ldots, x_n)$$

Concluding Remarks

- ILTS a general framework to talk about symbolic systems, vectorial systems, ... with general algorithm patterns for bisimulation, symbolic model-checking, etc. A multi-agents view generalizing control problems, ...
- The Sigali Tool

  The Control of Polynomial Dynamical Systems (in $\mathbb{Z}/3\mathbb{Z}$)

  Set Y splits into $K \cup U$ controllable and uncontrollable events variables

$$\left\{ \begin{array}{rcl} Q_0(X) & = & 0 \\ Q(X,Y) & = & X' \end{array} \right. \quad \leadsto \quad \left\{ \begin{array}{rcl} Q_0(X) \oplus C_0(X) & = & 0 \\ Q(X,Y) & = & X' \\ C(X,Y) & = & 0 \end{array} \right.$$

- For Reachability, Inevitability, Persistence, and Recurrence of a set of states