Specifying and Synthesizing
Open Systems and their Controllers

Sophie Pinchinat
MARIE CURIE FELLOW

Computer Sciences Laboratory - RSISE
The Australian National University
Canberra - Australia

IRISA - INRIA
Campus de Beaulieu
F-35042, Rennes - France

Sophie.Pinchinat@{irisa.fr,rsise.anu.edu.au}
Plan

- The Framework
- Model-Checking Closed Systems
- Satisfiability
- Synthesis of Decisions for $\varphi$ over $\Lambda$
- Expressing Qualitative Properties Decisions
- Expressing Constraints on Decisions
- Perspectives
- Partial Observation
The Framework

- A fixed set $\Sigma = \{a, b, c, \ldots\}$
- The full tree $T$
- A labeling $\lambda : \Sigma^* \to 2^\Lambda$ where $\Lambda$ is a set of propositions
- A decision is a labeling $p : \Sigma^* \to 2^p$ where $p$ is a proposition
Example

\[ \lambda : \{a, b\}^* \rightarrow 2^{\circ, q} \]

Use labels \( \circ \) and \( q \)
Example

\[ p : \Sigma^* \rightarrow 2^p \]
p : \Sigma^* \rightarrow 2^p

Example

\[(T, \lambda) \text{ in } p\]
The Logic

- **Mu-calculus** $\varphi \leadsto \varphi \text{IN} p$, modalities refer to trajectories “inside $p$”

\[
\begin{align*}
< a > \varphi \text{IN} p &= < a > (p \land \varphi \text{IN} p) \\
(\neg \varphi) \text{IN} p &= \neg (\varphi \text{IN} p) \\
(\mu Y. \varphi) \text{IN} p &= \mu Y. (\varphi \text{IN} p)
\end{align*}
\]

- **Theorem** $(T, \lambda) \text{IN} p \models \varphi$ iff $(T, \lambda) \models \varphi \text{IN} p$

- **Let** $S$ be represented by $(T, \lambda) \text{IN} \circ$ with $\Lambda \supseteq \{\circ\}

\[
S \models \varphi \text{ if and only if } (T, \lambda) \text{IN} \circ \models \varphi \text{ if and only if } (T, \lambda) \models \varphi \text{IN} \circ
\]
Model-Checking Closed Systems

Given $\lambda : \Sigma^* \rightarrow \Lambda$ and $\varphi$ over $\Lambda$

$$(T, \lambda) \models \varphi?$$

1) Provided $(T, \lambda)$ finitely represented ($\lambda$ is regular)
2) Consider the alternating (parity) tree automaton $A_\varphi$
3) Find a (memoryless) winning strategy in $G((T, \lambda), A_\varphi)$
Satisfiability of $\varphi$ over $\Lambda$

Does $(T, \lambda) \models \varphi$ for some $\lambda : \Sigma^* \rightarrow \Lambda$?

Find a memoryless w.s. in $G(\mathcal{A}_\varphi)$

$(T, \emptyset) \models \exists \Lambda. \varphi$?

1) Compute $B$ a ndta equivalent to $\mathcal{A}_\varphi$ Simulation Theorem
2) Get $B'$ by projecting $B$ in order to forget $\Lambda$
3) Find a memoryless w.s. in $G((T, \emptyset), B')$ delivering the propositions in $\Lambda$

Complexity: EXPTIME in $\varphi$ and PTIME in $\lambda$
Synthesizing a Decision for $\varphi$ over $\Lambda$

Does $(T, \lambda) \models \varphi$ for some decision $p$?

Does $(T, \lambda) \models \varphi$ in $p$ for some decision $p$?

$(T, \lambda) \models \exists p. \varphi$ in $p$?

1) Compute $B'$ as $A_{\varphi \models_p} \downarrow p$  
   Simulation Theorem

2) Find a memoryless w.s. in $G((T, \lambda), B')$ delivering the values of $p$

Complexity: EXPTIME in $\varphi$ and PTIME in $\lambda$
Expressing Qualitative Properties of the Decision $p$

$p \sqsubseteq p'$ \quad \begin{cases} \text{means labeled by } p \text{ implies labeled by } p' \\ \text{is } L_\mu \text{ definable} \end{cases}

Maximal permissiveness \quad (T, \lambda) \models \exists p. \varphi \text{ in } p \land \forall p'. [p \sqsubseteq p' \Rightarrow \neg \varphi \text{ in } p']

Minimal permissiveness

Uniqueness
Expressing Constraints on the Decision

Taking into account e.g. inputs, environment’s move, other players’, decision of other agents... Given by some “states”, some propositions or some events...

- Control of Closed systems $\Sigma_u \subseteq \Sigma$ uncontrollable events
  
  $$(T, \lambda) \models \exists p. \ AG(\bigwedge_{u \in \Sigma_u} <u>p) \land \varphi \text{ IN } p$$

- Module Checking/MC Open Systems $\{S, E\} \subseteq \Lambda$ exclusive
  
  $$(T, \lambda) \models \forall e. \ AG(S \Rightarrow \bigwedge_{a \in \Sigma}[a]e) \land \varphi \text{ IN } e$$

- Control of Open Systems/Computing Strategies
  
  $$(T, \lambda) \models \exists p. \ AG(E \Rightarrow \bigwedge_{a \in \Sigma}[a]p)$$
  
  $$\land \forall e. AG(S \Rightarrow \bigwedge_{a \in \Sigma}[a]e) \land \varphi \text{ IN } (p \land e)$$

Complexity: 2EXPTIME in $\varphi$ and PTIME in $\lambda$

Maximal Permissiveness 3EXPTIME
Model-Checking

\[ Q_1 \Lambda_1 . Q_2 \Lambda_2 . \ldots . Q_n \Lambda_n . \varphi \text{ is } |\lambda|^{(n-1)\text{EXP}(|\varphi|)} \times \text{EXP}(|\varphi|) \]

Satisfiability

\[
\begin{align*}
\exists \Lambda_1 . Q_2 \Lambda_2 . \ldots . Q_n \Lambda_n . \varphi & \text{ is } n\text{EXP}(|\varphi|) \\
\forall \Lambda_1 . Q_2 \Lambda_2 . \ldots . Q_n \Lambda_n . \varphi & \text{ is } (n + 1)\text{EXP}(|\varphi|)
\end{align*}
\]

Succinctness w.r.t. the mu-calculus
**Game Structures** with labelings. Take $A = \{1, 2\} \subseteq Agt = \{1, 2, 3\}$

$out(F_A, q)$ is given by 3 propositions $p_1$ (choice of gent 1), $p_2$, and $p_3$

$\langle\langle A, a\rangle\rangle \circ \varphi$ translates $\exists p_1 \exists p_2 \forall p_3. (<a>\varphi) \text{IN} (p_1 \land p_2 \land p_3)$

**Complexity Issue** (size a models)

**Components** Given classes $\gamma_1, \gamma_2, \gamma_3$ for components

$\exists p_1 \in \gamma_1. \forall p_2 \in \gamma_2. \forall p_3 \in \gamma_3. \varphi \text{IN} (p_1 \land p_2 \land p_3)$

**Fusioning Decisions**

$\exists p_1 \in \gamma_1. \exists p_2 \in \gamma_2. \forall p_3 \in \gamma_3. \varphi \text{IN} \alpha(p_1, p_2, p_3)$.

e.g. $\alpha(p_1, p_2, p_3) = p_1 \lor p_2 \lor p_3$

e.g. $\alpha(p_1, p_2, p_3) = p_1 \land <a>p_2 \land p_3$

**Expressiveness?**
Partial Observation

- Given $I \subseteq \Sigma$ of internal moves
  
  Define $\sim \subseteq \Sigma^*$ for the congruence generated by $\epsilon \sim i$ for all $i \in I$

- $(T, \lambda) \models \exists^\sim p. \varphi$ means \[
\begin{cases}
\text{there exists } p \text{ s.t. } (T, \lambda \cup p) \models \varphi, \text{ and} \\
\text{moreover } p(w) = p(w') \text{ whenever } w \sim w'
\end{cases}
\]

  $p$ is a uniform strategy

- The MC of $Q_1^1 p_1. Q_2^2 p_2 \cdots Q_m^m p_m. \varphi$ is decidable whenever $\sim_m \subseteq \cdots \subseteq \sim_2 \subseteq \sim_1$

  [Pinchinat&Riedweg05]

- Corollary (with $\sim_1 = \sim_2$) Maximal Permissiveness is decidable

- Corollary Open Systems under Partial Observation
More Regarding Partial Observation

- Interplay between labelings over the Full Trees $\Sigma' \cup \mathcal{I} \subseteq \Sigma$
  
  [Pinchinat&Riedweg05] Weak Synchronous Product
  
  [AVW03] [Briand06] Propositions $\otimes^i$ and Loop Automata

- Observational equivalences between labelings ($\tau$-bisimulations)
  
  Non-deterministic Models with deterministic decisions [Pinchinat&Raclet05]
  
  Undistinguishable moves as in [Briand06]

- Games to decide Observability Properties
  
  ★ Exhibit $w \sim w'$ but $w \in \text{Acc}$ and $w' \not\in \text{Acc}$
  
  ($w \sim_1 w_1$ and $w \sim_2 w_2$ but $w \in \text{Acc}$ and $w_1, w_2 \not\in \text{Acc}$)
  
  ★ Extend/Restrict a property to make it observable
  
  ★ Extend the perception to observe certain properties