How to decide qualitative properties for higher-order program with Nature?

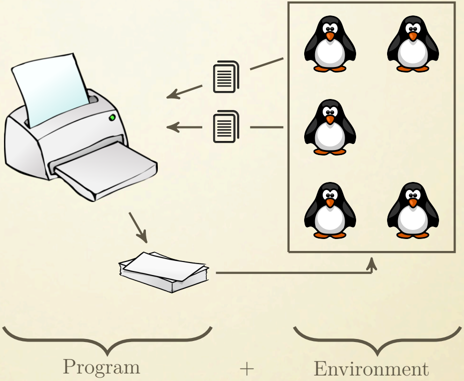
Arnaud Carayol [1] Olivier Serre [2]

[1]LIGM (Université Paris Est & CNRS)

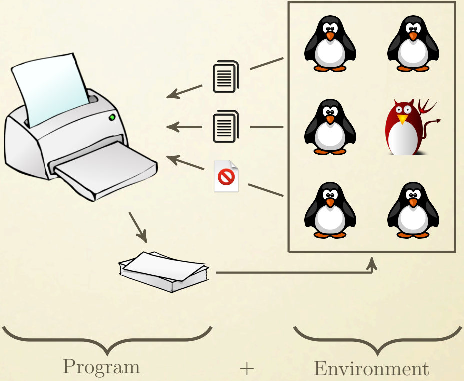
[2]IRIF (Université Paris Diderot – Paris 7 & CNRS)

HOMCS+CDPS workshop (IMS, September 2016)

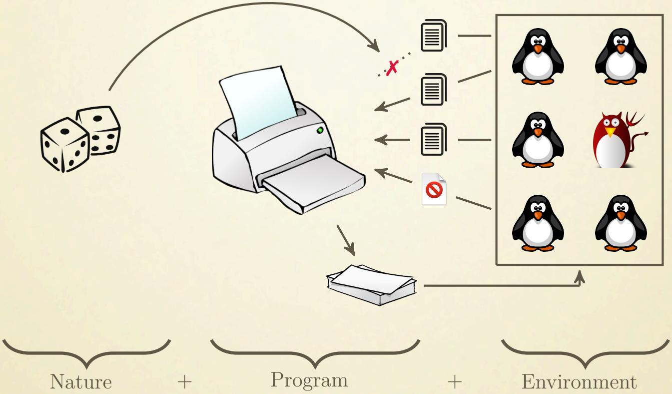
The General Context



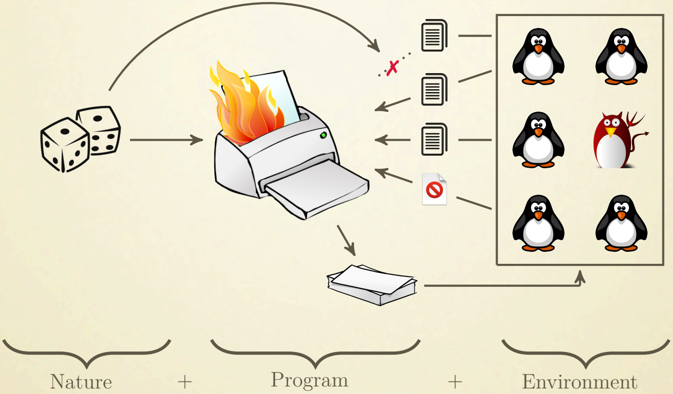
The General Context



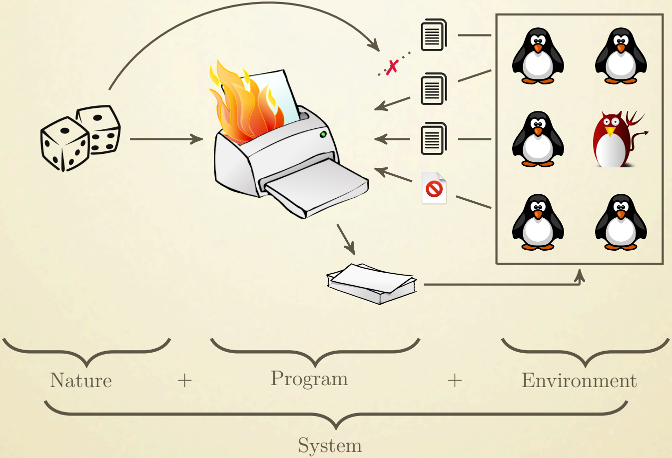
The General Context



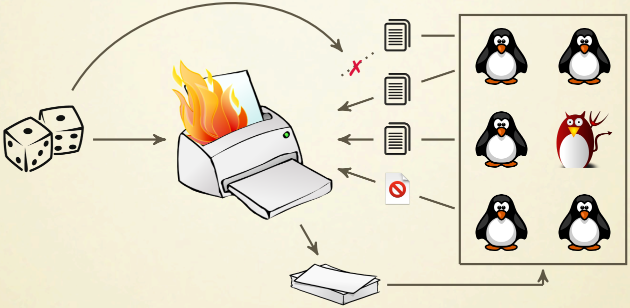
The General Context



The General Context



The General Context



Nature + Program + Environment

System

Specification: Every (valid) job gets eventually printed except in very unlikely executions?

Proposing tractable and robust definitions to capture negligible set of executions is at the heart of this work.

Games With Nature: Basic Definitions

Three players

- **Éloïse:** Standing for the program ➔ controllable.
- **Abélard:** Standing for the environment ➔ uncontrollable + possibly hostile.
- **Nature:** Standing for nature ➔ uncontrollable + unpredictable.

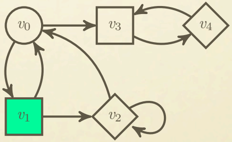
Games With Nature: Basic Definitions

Three players

- **Éloïse:** Standing for the program ➔ controllable.
- **Abélard:** Standing for the environment ➔ uncontrollable + possibly hostile.
- **Nature:** Standing for nature ➔ uncontrollable + unpredictable.

Game $\mathbb{G} = (\mathcal{A}, \Omega, v_0)$

- An **arena** $\mathcal{A}$: A directed graph $G = (V, E)$ whose vertices have been partitioned among the players.
- An **initial vertex** $v_0 \in V$.



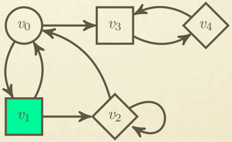
Games With Nature: Basic Definitions

Three players

- **Éloïse:** Standing for the program ➔ controllable.
- **Abélard:** Standing for the environment ➔ uncontrollable + possibly hostile.
- **Nature:** Standing for nature ➔ uncontrollable + unpredictable.

Game $\mathbb{G} = (\mathcal{A}, \Omega, v_0)$

- An **arena** $\mathcal{A}$: A directed graph $G = (V, E)$ whose vertices have been partitioned among the players.
- An **initial vertex** $v_0 \in V$.



- A pebble is put on v_0 and is moved along edges by the players.
- A **winning condition**: A (say Borel) subset Ω of V^ω.
- A play is an infinite path $\lambda \in V^\omega$: it is won by Éloïse if $\lambda \in \Omega$ and otherwise it is won by Abélard.

Games With Nature: Basic Definitions

Game $\mathbb{G} = (\mathcal{A}, \Omega, v_0)$

- An **arena** $\mathcal{A}$: A directed graph $G = (V, E)$ whose vertices have been partitioned among the players.
- An **initial vertex** $v_0 \in V$.
- A pebble is put on v_0 and is moved along edges by the players.
- A **winning condition**: A (say Borel) subset Ω of V^ω.
- A play is an infinite path $\lambda \in V^\omega$: it is won by Éloïse if $\lambda \in \Omega$ and otherwise it is won by Abélard.

Popular winning conditions:

- Reachability condition: Éloïse wins if a final state is eventually reached, *i.e.* $\Omega = V^* F V^\omega$.
- Büchi condition: Éloïse wins if final states are infinitely often visited, *i.e.* $\Omega = \cap_{i \geq 0} V^i V^* F V^\omega$.
- Parity condition: Every vertex gets a colour from a *finite* set; Éloïse wins if the smallest colour infinitely often visited is even.

Handling Higher-Order Programs

The general roadmap:

1. Abstract the system as a scheme.
2. Build an equivalent collapsible pushdown automaton.
3. Reflect who does what using the control states of the CPDA (a state is controlled by Éloïse, Abélard or Nature).

Special case:

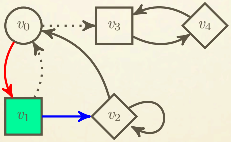
1. Closed system (*i.e.* no environment): no Abélard.
2. No unpredictable uncontrollable state: no Nature.

Possible extra features: imperfect information, *e.g.* when having public/private variables.

Games With Nature: Strategies

Strategies

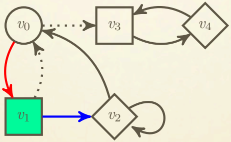
- A strategy for Éloïse is a map $\varphi_E : V^* V_E \to V$.
- A strategy for Abélard is a map $\varphi_A : V^* V_A \to V$.
- Nature is fully non-deterministic hence, does not use strategies.



Games With Nature: Strategies

Strategies

- A strategy for Éloïse is a map $\varphi_E : V^* V_E \to V$.
- A strategy for Abélard is a map $\varphi_A : V^* V_A \to V$.
- Nature is fully non-deterministic hence, does not use strategies.



➔ Given (φ_E, φ_A) one gets a set $\mathrm{Outcomes}_{v_0}^{\varphi_E,\varphi_A}$ of all plays where Éloïse/Abélard respects her/his strategy.

Remark. One can think of $\mathrm{Outcomes}_{v_0}^{\varphi_E,\varphi_A}$ as the set of branches of the tree of partial plays where the players respect their strategies.

Games Without Nature (aka 2-Player Games)

Things work fine:

- For Borel winning conditions Ω the games are *determined*: Either Éloïse or Abélard has a winning strategy:

$$\exists\varphi_{\mathrm{E}}\forall\varphi_{\mathrm{A}}\ \mathrm{Outcomes}_{v_0}^{\varphi_E,\varphi_A} \subseteq \Omega \quad \textbf{or} \quad \exists\varphi_{\mathrm{A}}\forall\varphi_{\mathrm{E}}\ \mathrm{Outcomes}_{v_0}^{\varphi_E,\varphi_A} \cap \Omega = \emptyset$$

- For parity winning conditions, winning strategies can be chosen positional (*i.e.* as map from $V \to V$).
- For ω-regular winning conditions one can decide who has a winning strategy and compute winning strategies for a large class of graphs: finite ones, pushdown graphs, collapsible pushdown graphs.

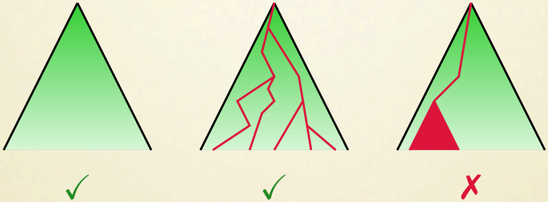
Consequence for program verification:

- One can do model-checking (and even program synthesis) for higher-order programs against ω-regular specifications

Games With Nature
Evaluating a Situation/Strategy

How good is strategy φ_E against strategy φ_A?

➔ Look how “small” is the set of loosing plays for Eloise.

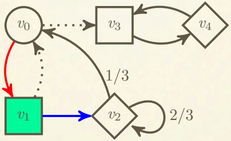


How good is strategy φ_E?

➔ Look how good is φ_E in the worse case (*i.e.* against the best counter-strategy φ_A of Abélard).

The Probabilistic Setting (Stochastic Games)

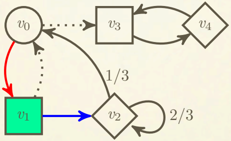
- Nature is coming with a probabilistic semantics.



- A pair of strategies (φ_E, φ_A) induces a probability measure $\mu_{v_0}^{\varphi_E,\varphi_A}$ on $\mathrm{Outcomes}_{v_0}^{\varphi_E,\varphi_A}$.
- $\mathrm{Val}_{\mathbb{G}}(\varphi_{\mathrm{E}}) = \inf\{\mu_{v_0}^{\varphi_{\mathrm{E}},\varphi_{\mathrm{A}}}(\Omega) \mid \varphi_{\mathrm{A}}$ Abélard strategy$\}$.
- $\mathrm{Val}(\mathbb{G}) = \sup\{\mathrm{Val}_{\mathbb{G}}(\varphi_{\mathrm{E}}) \mid \varphi_{\mathrm{E}}$ Éloïse strategy$\}$.
- Typical (qualitative) questions: does $\mathrm{Val}(\mathbb{G}) = 1$? If so is there an optimal strategy, *i.e.* a φ_E such that $\mathrm{Val}_{\mathbb{G}}(\varphi_{\mathrm{E}}) = 1$?

The Probabilistic Setting (Stochastic Games)

- Nature is coming with a probabilistic semantics.



- A pair of strategies (φ_E, φ_A) induces a probability measure $\mu_{v_0}^{\varphi_E,\varphi_A}$ on $\text{Outcomes}_{v_0}^{\varphi_E,\varphi_A}$.
- $\text{Val}_{\mathbb{G}}(\varphi_{\text{E}}) = \inf\{\mu_{v_0}^{\varphi_{\text{E}},\varphi_{\text{A}}}(\Omega) \mid \varphi_{\text{A}}$ Abélard strategy$\}$.
- $\text{Val}(\mathbb{G}) = \sup\{\text{Val}_{\mathbb{G}}(\varphi_{\text{E}}) \mid \varphi_{\text{E}}$ Éloïse strategy$\}$.
- Typical (qualitative) questions: does $\text{Val}(\mathbb{G}) = 1$? If so is there an optimal strategy, *i.e.* a φ_E such that $\text{Val}_{\mathbb{G}}(\varphi_{\text{E}}) = 1$?

➔ **Well-understood (and decidable)** when arena is finite + Ω is ω-regular + perfect information. In other situations: quickly becomes **undecidable**.

The Probabilistic Setting for Programs With (Higher-Order)-Recursion

(Un)Decidability landscape:

- When Nature is not involved parity games on CPDA graphs are decidable [HMOS08] + finite effective presentation of the winning region [BCOS10] + effective winning strategies [CS12].
- When Nature is involved and even if Abélard is not: undecidable even for reachability (except under strong restrictions) [EY05].

The Probabilistic Setting for Programs With (Higher-Order)-Recursion

(Un)Decidability landscape:

- When Nature is not involved parity games on CPDA graphs are decidable [HMOS08] + finite effective presentation of the winning region [BCOS10] + effective winning strategies [CS12].
- When Nature is involved and even if Abélard is not: undecidable even for reachability (except under strong restrictions) [EY05].

End of the story?

The Probabilistic Setting for Programs With (Higher-Order)-Recursion

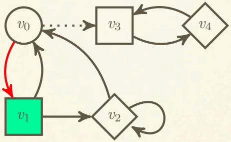
(Un)Decidability landscape:

- When Nature is not involved parity games on CPDA graphs are decidable [HMOS08] + finite effective presentation of the winning region [BCOS10] + effective winning strategies [CS12].
- When Nature is involved and even if Abélard is not: undecidable even for reachability (except under strong restrictions) [EY05].

End of the story?

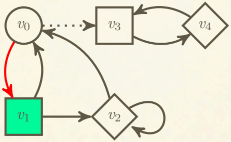
➔Not really... One should just fine alternative ways to define negligible sets of executions!

Using Cardinality to Define Negligible Sets



Remark. For any strategy of Abélard, Éloïse (using the red arrow) wins all plays but a countable number.

Using Cardinality to Define Negligible Sets

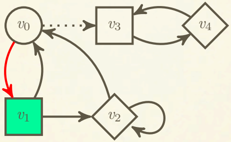


Remark. For any strategy of Abélard, Éloïse (using the red arrow) wins all plays but a countable number.

➔ Go back to a **non-deterministic** semantics for Nature and count number of loosing plays.

- $\mathit{CardLeak}(\varphi_{\mathrm{E}}) = \sup\{\mathit{Card}(\mathrm{Outcomes}_{v_0}^{\varphi_{\mathrm{E}},\varphi_{\mathrm{A}}} \setminus \Omega) \mid \varphi_{\mathrm{A}} \text{ Abélard's strat}\}$.
- $\mathit{LeakVal}(\mathbb{G}) = \inf\{\mathit{CardLeak}(\varphi_{\mathrm{E}}) \mid \varphi_{\mathrm{E}} \text{ strategy of Éloïse}\}$.

Using Cardinality to Define Negligible Sets



Remark. For any strategy of Abélard, Éloïse (using the red arrow) wins all plays but a countable number.

➔ Go back to a **non-deterministic** semantics for Nature and count number of loosing plays.

- $\mathit{CardLeak}(\varphi_{\mathrm{E}}) = \sup\{\mathit{Card}(\mathrm{Outcomes}_{v_0}^{\varphi_{\mathrm{E}},\varphi_{\mathrm{A}}} \setminus \Omega) \mid \varphi_{\mathrm{A}}$ Abélard's strat$\}$.
- $\mathit{LeakVal}(\mathbb{G}) = \inf\{\mathit{CardLeak}(\varphi_{\mathrm{E}}) \mid \varphi_{\mathrm{E}}$ strategy of Éloïse$\}$.

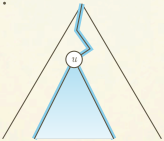
Proposition. $\mathit{LeakVal}(\mathbb{G}) \in \mathbb{N} \cup \{\aleph_0, 2^{\aleph_0}\}$.

Proposition. Optimal strategies for Éloïse always exist.

Using Topology to Define Negligible Sets

The set of branches in a tree as a topological space.

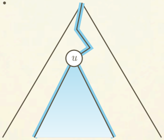
- Basic open sets: the cones.



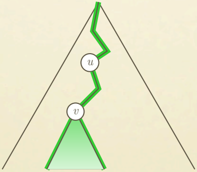
Using Topology to Define Negligible Sets

The set of branches in a tree as a topological space.

- Basic open sets: the cones.



- A set of branches B is **nowhere dense** if for all node u, there exists a descendant v of u such that no branch of B goes through v.

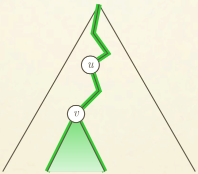


- A set of branches is **meagre** if it is the countable union of nowhere dense sets.

Using Topology to Define Negligible Sets

The set of branches in a tree as a topological space.

• A set of branches B is **nowhere dense** if for all node u, there exists a descendant v of u such that no branch of B goes through v.



• A set of branches is **meagre** if it is the countable union of nowhere dense sets.

➔ Go back to a **non-deterministic** semantics for Nature and look whether the set of loosing plays is meager.

Definition. φ_{E} is **topologically good** if and only if *for any* strategy φ_{A} of Abélard the set $\mathrm{Outcomes}_{v_0}^{\varphi_{\mathrm{E}},\varphi_{\mathrm{A}}} \setminus \Omega$ is meager.

What Kind of Results Did We Prove?

We want to decide, for a given game with nature $\mathbb{G}$, the following problems:

(1) Does one has $LeakVal(\mathbb{G}) \leq \aleph_0$?

(2) Has Éloïse a topologically good strategy?

What Kind of Results Did We Prove?

We want to decide, for a given game with nature $\mathbb{G}$, the following problems:

(1) Does one has $\mathit{LeakVal}(\mathbb{G}) \leq \aleph_0$?

(2) Has Éloïse a topologically good strategy?

We give transformations that associate with any game with Nature $\mathbb{G} = (\mathcal{A}, \Omega, v_0)$ a game **without** Nature $\widehat{\mathbb{G}} = (\widehat{\mathcal{A}}, \widehat{\Omega}, \widehat{v_0})$ on which question (1)/(2) is restated as whether Éloïse has a winning strategy.

- $\widehat{\mathcal{A}}$: $\mathcal{A}$ + gadgets
- $\widehat{\Omega}$: Simple Boolean combination of Ω with an ω-regular condition

What Kind of Results Did We Prove?

We want to decide, for a given game with nature $\mathbb{G}$, the following problems:

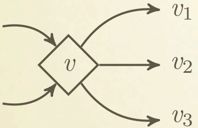
(1) Does one has $\mathit{LeakVal}(\mathbb{G}) \leq \aleph_0$?

(2) Has Éloïse a topologically good strategy?

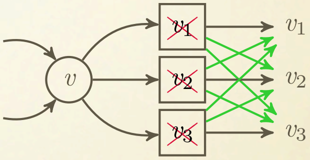
We give transformations that associate with any game with Nature $\mathbb{G} = (\mathcal{A}, \Omega, v_0)$ a game **without** Nature $\widehat{\mathbb{G}} = (\widehat{\mathcal{A}}, \widehat{\Omega}, \widehat{v_0})$ on which question (1)/(2) is restated as whether Éloïse has a winning strategy.

- $\widehat{\mathcal{A}}$: $\mathcal{A}$ + gadgets
- $\widehat{\Omega}$: Simple Boolean combination of Ω with an ω-regular condition
- Extra hypothesis:
  - $\mathit{LeakVal}(\mathbb{G}) \leq \aleph_0$? No extra hypothesis on $\mathbb{G}$
  - Existence of topo. good strategies: **Éloïse + Nature only**

The gadget:



Game $\mathbb{G}$

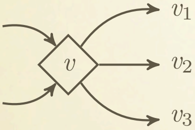


Game $\widehat{\mathbb{G}}$

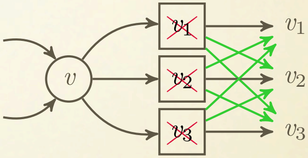
$\hat{\Omega} = \Omega \vee$ **finitely many green edges**

Leaking Value | Perfect-Information Setting

The gadget:



Game $\mathbb{G}$



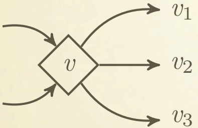
Game $\widehat{\mathbb{G}}$

$\hat{\Omega} = \Omega \vee$ **finitely many green edges**

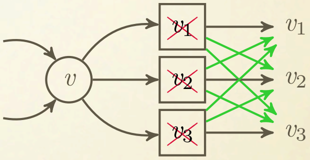
Theorem. $\mathit{LeakVal}(\mathbb{G}) \leq \aleph_0$ iff Éloïse has a winning strategy in $\widehat{\mathbb{G}}$.

Leaking Value | Perfect-Information Setting

The gadget:



Game $\mathbb{G}$



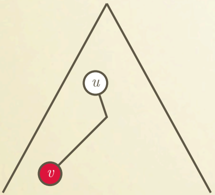
Game $\widehat{\mathbb{G}}$

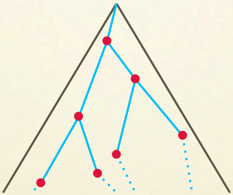
$\hat{\Omega} = \Omega \vee$ **finitely many green edges**

Theorem. $\mathit{LeakVal}(\mathbb{G}) \leq \aleph_0$ iff Éloïse has a winning strategy in $\widehat{\mathbb{G}}$.

Proposition. If $\mathbb{G}$ is a CPDA game then so is $\widehat{\mathbb{G}}$.

A set of nodes $W \subseteq \{0,1\}^*$ is *dense* if for every node $u \in \{0,1\}^*$ there exists $v \in W$ with $u \sqsubseteq v$. With such a W associate the set $\mathcal{B}(W)$ of branches that have infinitely many prefixes in W.

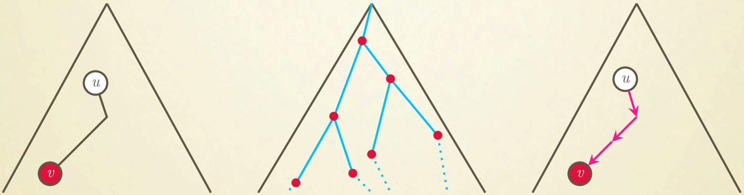




Lemma. A Borel set B of branches is large if and only if there exists W dense such that $\mathcal{B}(W) \subseteq B$.

Topo. Good Strategies | Perfect-Inf. Setting

A set of nodes $W \subseteq \{0,1\}^*$ is *dense* if for every node $u \in \{0,1\}^*$ there exists $v \in W$ with $u \sqsubseteq v$. With such a W associate the set $\mathcal{B}(W)$ of branches that have infinitely many prefixes in W.



Lemma. A Borel set B of branches is large if and only if there exists W dense such that $\mathcal{B}(W) \subseteq B$.

A direction mapping is a map $d : \{0,1\}^* \to \{0,1\}$. It points to W if following the directions indicated by the mapping starting from any node one ends up in a node in W.

Lemma. A set of nodes W is dense if and only if there exists a direction mapping that points to W.

Topo. Good Strategies | Perfect-Inf. Setting

A direction mapping is a map $d : \{0,1\}^* \to \{0,1\}$. It points to W if following the directions indicated by the mapping starting from any node one ends up in a node in W.

Lemma. A set of nodes W is dense if and only if there exists a direction mapping that points to W.

Starting from an Éloïse-Nature game $\mathbb{G}$ we build an Éloïse-Abélard game $\widehat{\mathbb{G}}$ where they mimics a play in $\mathbb{G}$ and where

- Éloïse provides a direction mapping to a set of nodes W
- Abélard simulates the moves of Nature and try to either prove that W is not dense or that there is a loosing play in $\mathcal{B}(W)$.

Theorem. Éloïse has a topologically good strategy in $\mathbb{G}$ iff Éloïse has a winning strategy in $\widehat{\mathbb{G}}$.

A direction mapping is a map $d : \{0,1\}^* \to \{0,1\}$. It points to W if following the directions indicated by the mapping starting from any node one ends up in a node in W.

Lemma. A set of nodes W is dense if and only if there exists a direction mapping that points to W.

Starting from an Éloïse-Nature game $\mathbb{G}$ we build an Éloïse-Abélard game $\widehat{\mathbb{G}}$ where they mimics a play in $\mathbb{G}$ and where

- Éloïse provides a direction mapping to a set of nodes W
- Abélard simulates the moves of Nature and try to either prove that W is not dense or that there is a loosing play in $\mathcal{B}(W)$.

Theorem. Éloïse has a topologically good strategy in $\mathbb{G}$ iff Éloïse has a winning strategy in $\widehat{\mathbb{G}}$.

Proposition. If $\mathbb{G}$ is a CPDA game then so is $\widehat{\mathbb{G}}$.

Consequences for Higher-Order Programs

Higher-order systems composed of: Program + Environment + Nature:

- For ω-regular specification everything (local/global model-checking + synthesis) works fine w.r.t the counting semantics.
- For ω-regular specification with no environment everything works fine w.r.t the topological semantics.

Consequences for Higher-Order Programs

Higher-order systems composed of: Program + Environment + Nature:

- For ω-regular specification everything (local/global model-checking + synthesis) works fine w.r.t the counting semantics.
- For ω-regular specification with no environment everything works fine w.r.t the topological semantics.

Is this relevant? Yes because...

- For finite MDP with ω-regular objective the probabilistic and the topological semantics coincide.

The Imperfect Information Setting

The Setting

- Set of vertices comes with an equivalence class $\sim$
- Éloïse only observes the equivalence class of the current states
- Éloïse plays actions and Nature resolves the non-determinism
- Abélard is perfectly informed: he plays as previously

The Imperfect Information Setting

The Setting

- Set of vertices comes with an equivalence class $\sim$
- Éloïse only observes the equivalence class of the current states
- Éloïse plays actions and Nature resolves the non-determinism
- Abélard is perfectly informed: he plays as previously

Again a pair of strategies $(\varphi_{\mathrm{E}}, \varphi_{\mathrm{A}})$ leads a tree of possible outcomes and one defines leaking value and topologically good strategies in the same spirit.

The Imperfect Information Setting

The Setting

- Set of vertices comes with an equivalence class $\sim$
- Éloïse only observes the equivalence class of the current states
- Éloïse plays actions and Nature resolves the non-determinism
- Abélard is perfectly informed: he plays as previously

Again a pair of strategies $(\varphi_{\mathrm{E}}, \varphi_{\mathrm{A}})$ leads a tree of possible outcomes and one defines leaking value and topologically good strategies in the same spirit.

We give transformations that associate with any game with Nature $\mathbb{G} = (\mathcal{A}, \Omega, v_0)$ a game **without** Nature $\widehat{\mathbb{G}} = (\widehat{\mathcal{A}}, \widehat{\Omega}, \widehat{v_0})$ on which previous questions are restated as whether Éloïse has a winning strategy.

- $\widehat{\mathcal{A}}$: $\mathcal{A}$ + gadgets (**preserves CPDA graphs**)
- $\widehat{\Omega}$: Simple Boolean combination of Ω and an ω-regular condition
- Extra hypothesis:
  - $\mathit{LeakVal}(\mathbb{G}) \leq \aleph_0$? Abélard perfect + Ω parity
  - Existence of topo. good strategies: Éloïse-Nature only + Ω parity

Summary

Main contributions

- New semantics for games with Nature.
- Leads to decidability results in many situations where the stochastic semantics was undecidable, including when handling higher-order programs.
- Several consequences.

Perspectives

- Applications? Find a convincing example...
- Logical counterparts?
- Extensions (in particular in the topological setting)?