Deciding the value 1 problem in 1-clock Decision Stochastic Timed Automata

Nathalie Bertrand[1] Thomas Brihaye[2] Blaise Genest[3]

[1] Inria & IRISA, Rennes, France

[2] Université Mons, Mons, Belgium

[3] CNRS, UMR IRISA, Rennes, France

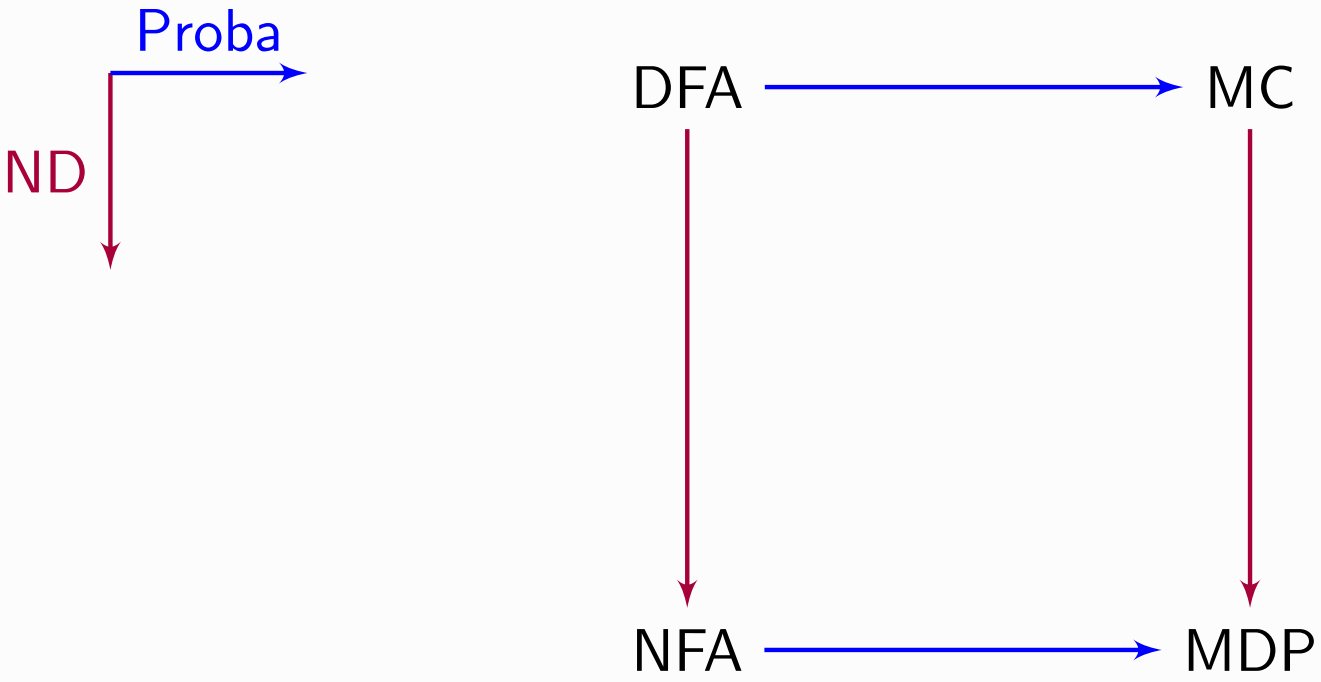
Third CASSTING meeting – Bruxelles – 21st May 2014

Modeling complex systems

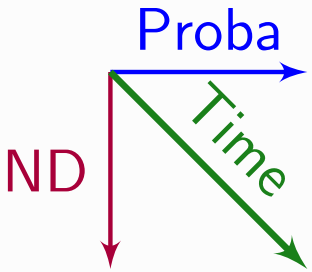
DFA

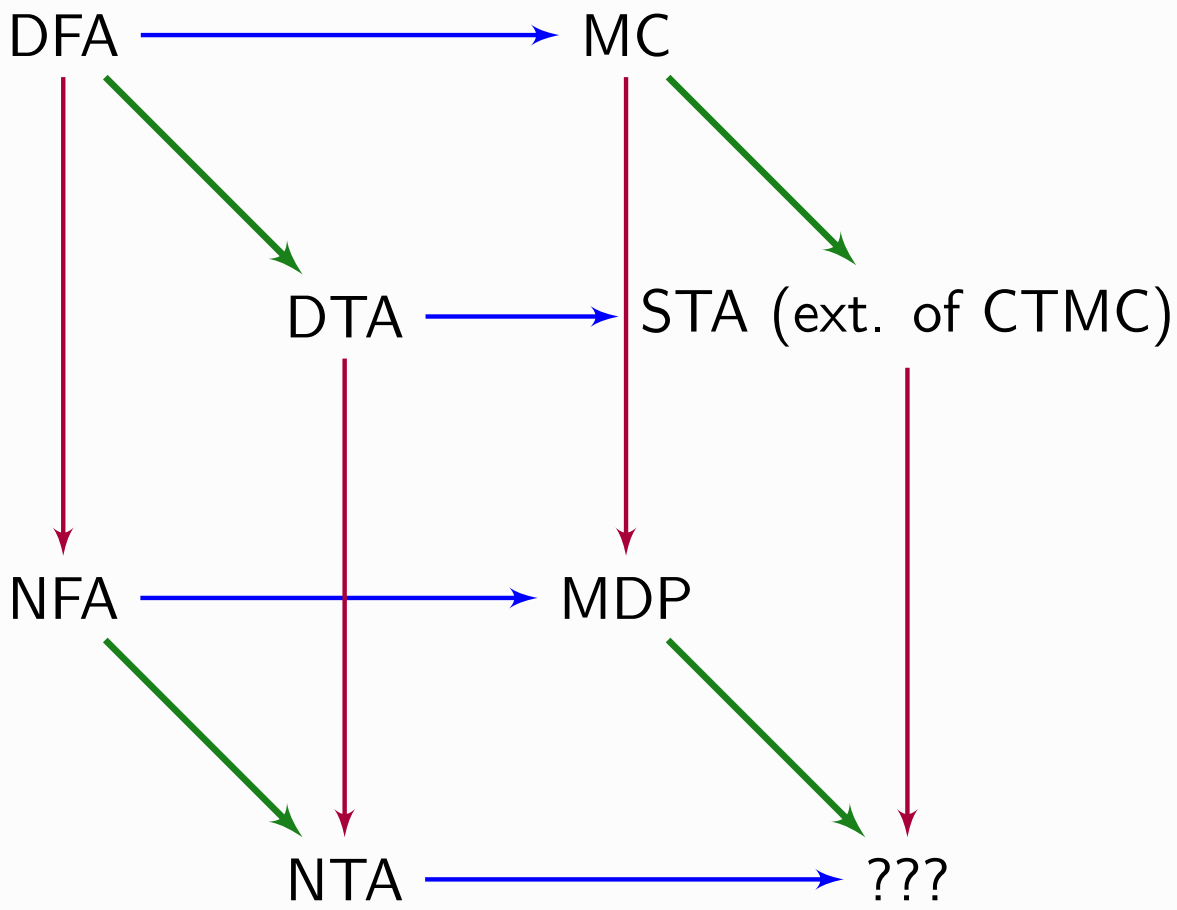
Modeling complex systems

Modeling complex systems



Modeling complex systems





Non-deterministic and probabilistic timed systems

Two approaches to combine probability, non-determinism and time:

- Probabilistic Timed Automata

  M. Z. Kwiatkowska, G. Norman, R. Segala, J. Sproston:
  Automatic Verification of Real-Time Systems with Discrete Probability Distributions. ARTS 1999

  - Time-delays are chosen non-deterministically,
  - Edges are according to discrete probability distributions.

- Decision Stochastic Timed Automata (ext. of CTMDP)

  Nathalie Bertrand, Sven Schewe:
  Playing Optimally on Timed Automata with Random Delays. FORMATS 2012

  - Time-delays are chosen via continuous probability distributions,
  - Edges are chosen non-deterministically.

Known results on (D)STA

Regarding STA

- The almost-sure model-checking of LTL is **decidable**
  - on 1-clock STA.

    C. Baier, N. Bertrand, P. Bouyer, T. Brihaye,M. Größer:
    Almost-Sure Model Checking of Infinite Paths in One-Clock Timed Automata. LICS 2008
  - on reactive n-clock STA.

    P. Bouyer, T. Brihaye, M. Jurdzinski, Q. Menet:
    Almost-Sure Model-Checking of Reactive Timed Automata. QEST 2012
- **No result** regarding the decidability of the almost-sure reachability problem on general 2-clock STA.

Regarding DSTA

- **Existence** of an optimal scheduler for the **time-bounded reachability problem** on reactive DSTA.

  Nathalie Bertrand, Sven Schewe:
  Playing Optimally on Timed Automata with Random Delays. FORMATS 2012

Known results on (D)STA

Regarding STA

- The almost-sure model-checking of LTL is **decidable**
  - on 1-clock STA.

    C. Baier, N. Bertrand, P. Bouyer, T. Brihaye,M. Größer:
    Almost-Sure Model Checking of Infinite Paths in One-Clock Timed Automata. LICS 2008
  - on reactive n-clock STA.

    P. Bouyer, T. Brihaye, M. Jurdzinski, Q. Menet:
    Almost-Sure Model-Checking of Reactive Timed Automata. QEST 2012
- **No result** regarding the decidability of the almost-sure reachability problem on general 2-clock STA.

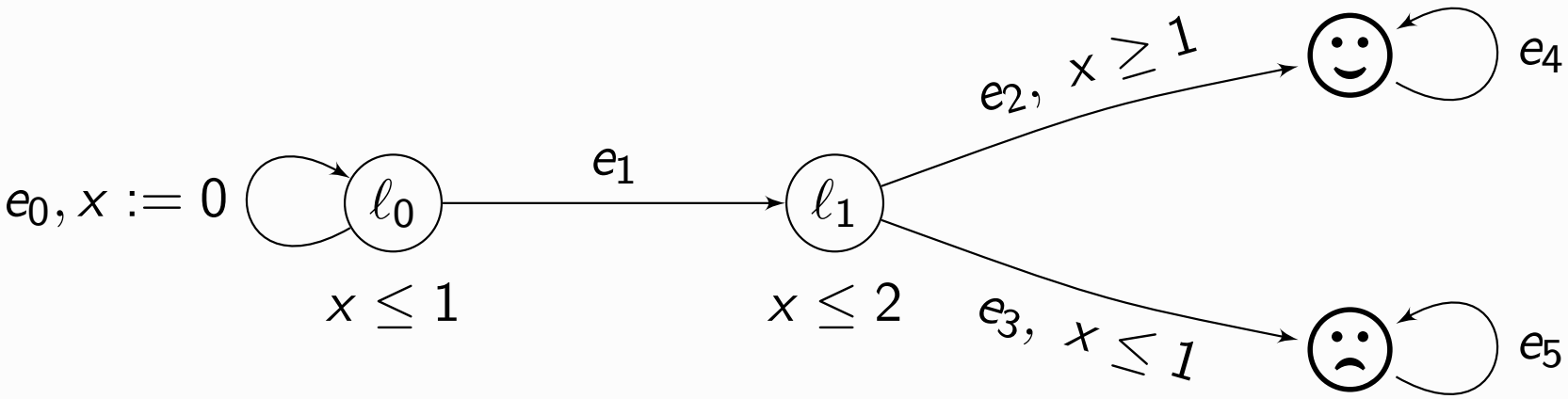
Regarding DSTA

- **Existence** of an optimal scheduler for the **time-bounded reachability problem** on reactive DSTA.

  Nathalie Bertrand, Sven Schewe:
  Playing Optimally on Timed Automata with Random Delays. FORMATS 2012

In this talk, we consider **reachability problem on 1-clock DSTA**.

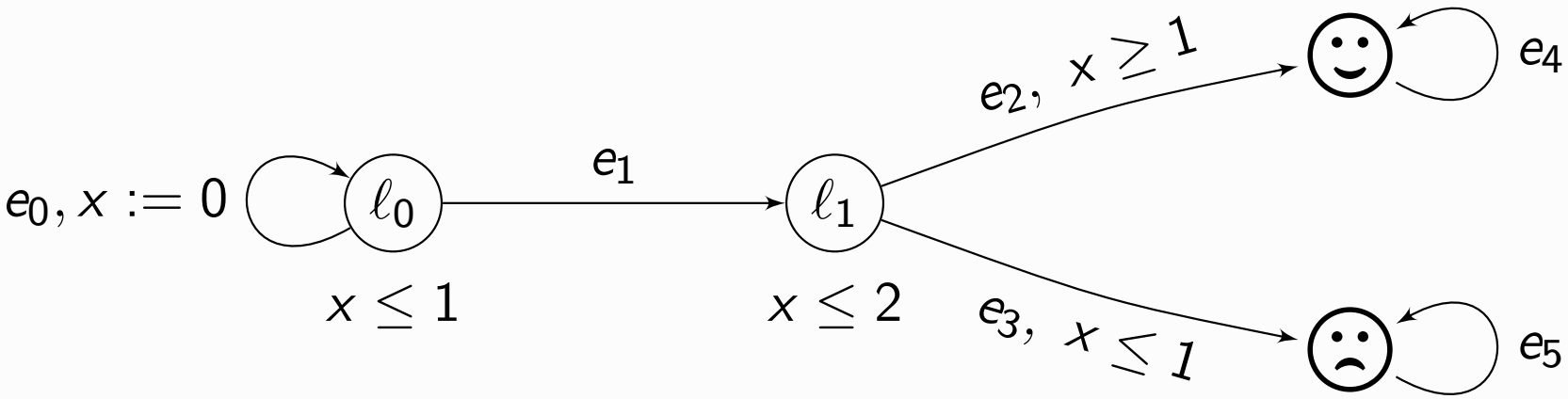
One-clock Timed Automaton



Definition

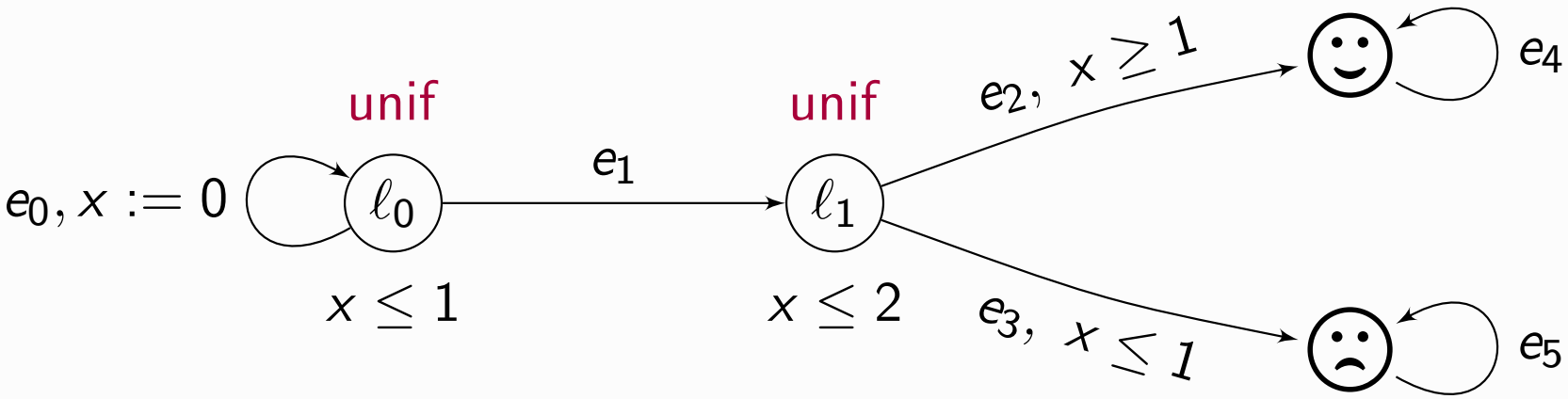
A **one-clock timed automaton** is a tuple $\mathcal{A} = (L, \ell_0, E, \mathcal{I})$ where:
(i) L is a finite set of locations, (ii) $\ell_0 \in L$ is the initial location,
(iii) $E \subseteq L \times \mathcal{G}(x) \times 2^{\{x\}} \times L$ is a finite set of edges, and
(iv) $\mathcal{I} : L \to \mathcal{G}(x)$ assigns an invariant to each location.

Semantics of TA



$$(\ell_0, 0) \xrightarrow{.7} (\ell_0, .7) \xrightarrow{e_0} (\ell_0, 0) \xrightarrow{.8} (\ell_0, .8) \xrightarrow{e_1} (\ell_1, .8) \xrightarrow{.3} (\ell_0, 1.1) \xrightarrow{e_2} \text{☺}$$

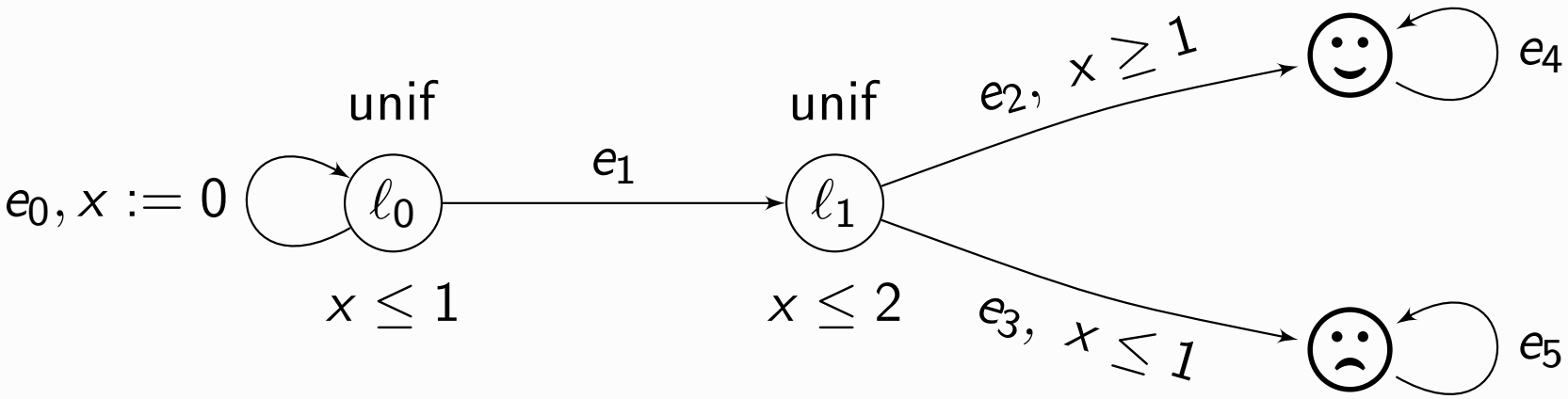
One-clock Decision Stochastic Timed Automaton



Definition

A **decision stochastic timed automaton** is a tuple $(\mathcal{A}, \mu)$, where
(i) $\mathcal{A} = (L, \ell_0, E, \mathcal{I})$ is a single clock timed automaton and
(ii) $\mu = (\mu_{\ell,t})$ is a family of *distributions*, $\mu_{\ell,t} \in \mathrm{Dist}(\mathcal{I}(\ell) \cap [t, +\infty[)$.

Semantics of DSTA - Intuitively

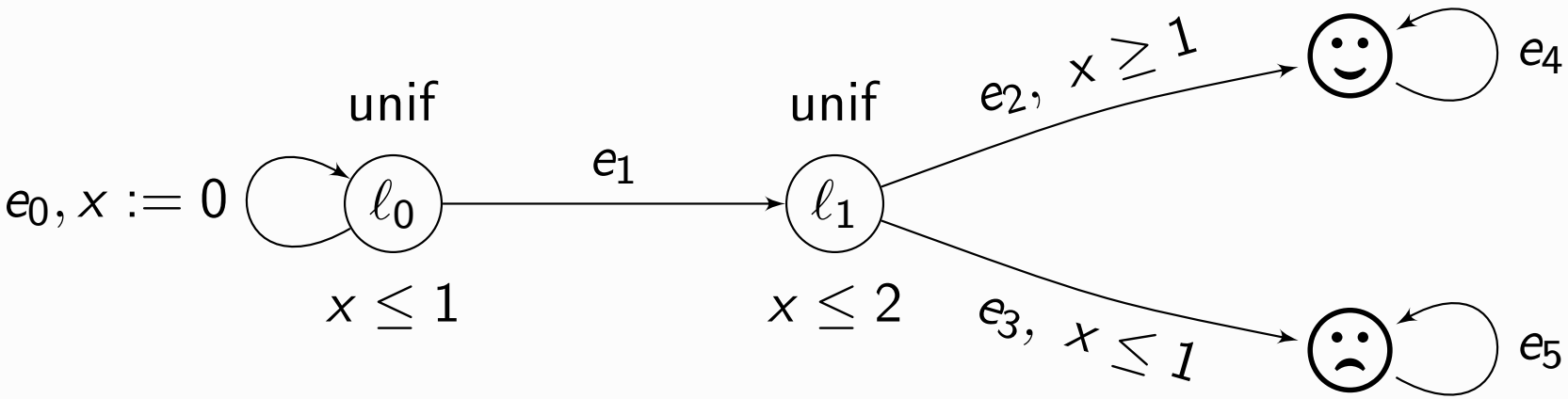


We consider an infinite state 1-1/2 player game. From a state s

- The *stochastic player* chooses randomly a delay τ (according to μ_s).
- The *non-deterministic player* chooses an edge e (enable from $s + \tau$).

We will denote by σ a **strategy of the non-deterministic player**.

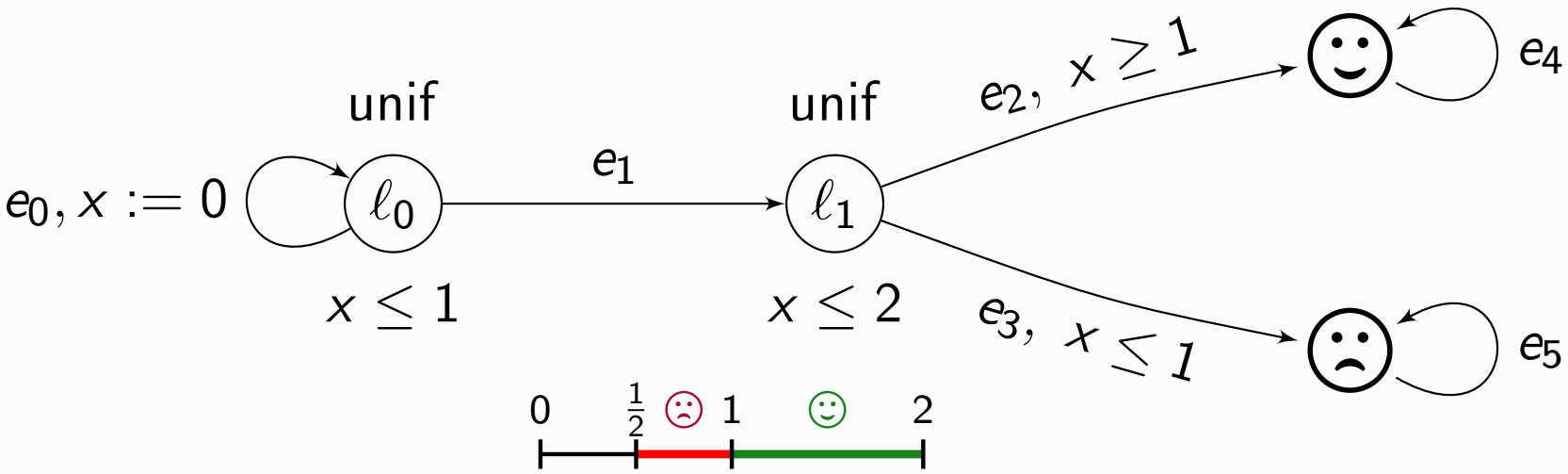
Examples of strategies (1)



$$\sigma(\ell_0, \nu) = \begin{cases} e_0 & \text{if } \nu < 1 \\ e_1 & \text{if } \nu = 1 \end{cases} \quad ; \quad \sigma(\ell_1, \nu) = \begin{cases} e_2 & \text{if } \nu \geq 1 \\ e_3 & \text{if } \nu < 1 \end{cases}$$

$$\mathbb{P}_\sigma^{s_0}\left((\mathcal{A}, \mu) \models \Diamond ☺\right) = 0, \qquad \text{where } s_0 = (\ell_0, 0).$$

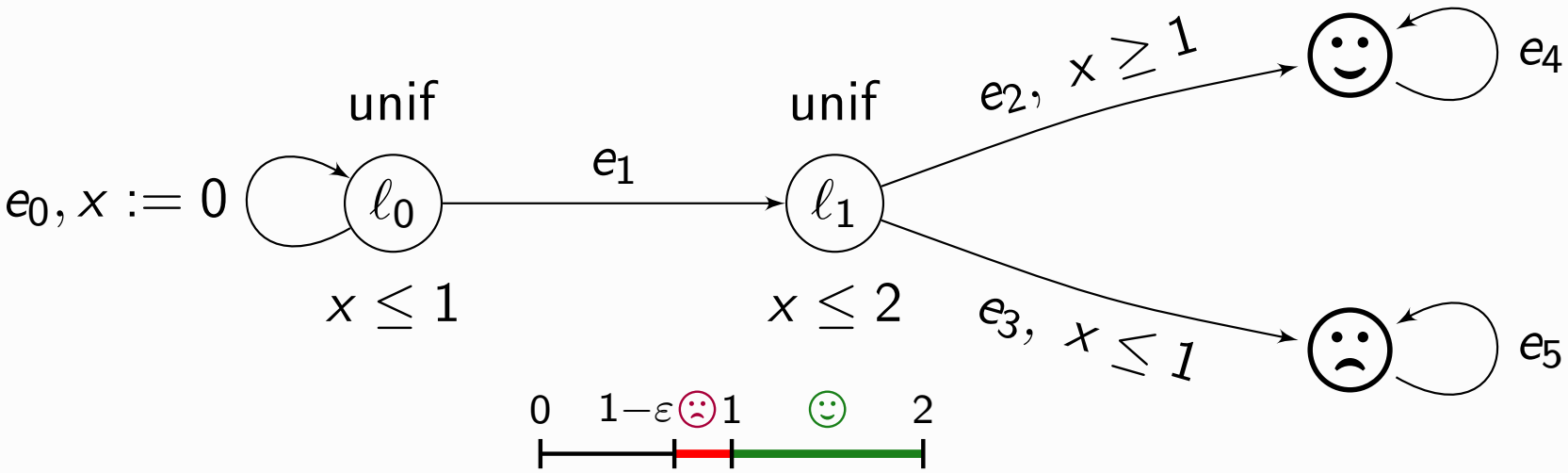
Examples of strategies (2)



$$\sigma'(\ell_0, \nu) = \begin{cases} e_0 & \text{if } \nu < \frac{1}{2} \\ e_1 & \text{if } \nu \geq \frac{1}{2} \end{cases} \quad ; \quad \sigma'(\ell_1, \nu) = \begin{cases} e_2 & \text{if } \nu \geq 1 \\ e_3 & \text{if } \nu < 1 \end{cases}$$

$$\mathbb{P}^{s_0}_{\sigma'}\left((\mathcal{A}, \mu) \models \Diamond ☺\right) \geq \frac{2}{3}, \qquad \text{where } s_0 = (\ell_0, 0).$$

Examples of strategies (3)



$$\sigma_\varepsilon(\ell_0, \nu) = \begin{cases} e_0 & \text{if } \nu < 1-\varepsilon \\ e_1 & \text{if } \nu \geq 1-\varepsilon \end{cases} \quad ; \quad \sigma_\varepsilon(\ell_1, \nu) = \begin{cases} e_2 & \text{if } \nu \geq 1 \\ e_3 & \text{if } \nu < 1 \end{cases}$$

$$\mathbb{P}^{s_0}_{\sigma_\varepsilon}\left((\mathcal{A}, \mu) \models \Diamond \text{☺}\right) \geq \frac{1}{1+\varepsilon} \geq 1-\varepsilon, \qquad \text{where } s_0 = (\ell_0, 0).$$

Almost-sure Vs Limit-sure

Given a DSTA $(\mathcal{A}, \mu)$, a target set $F \subseteq L$ and an initial state $s \in S$.

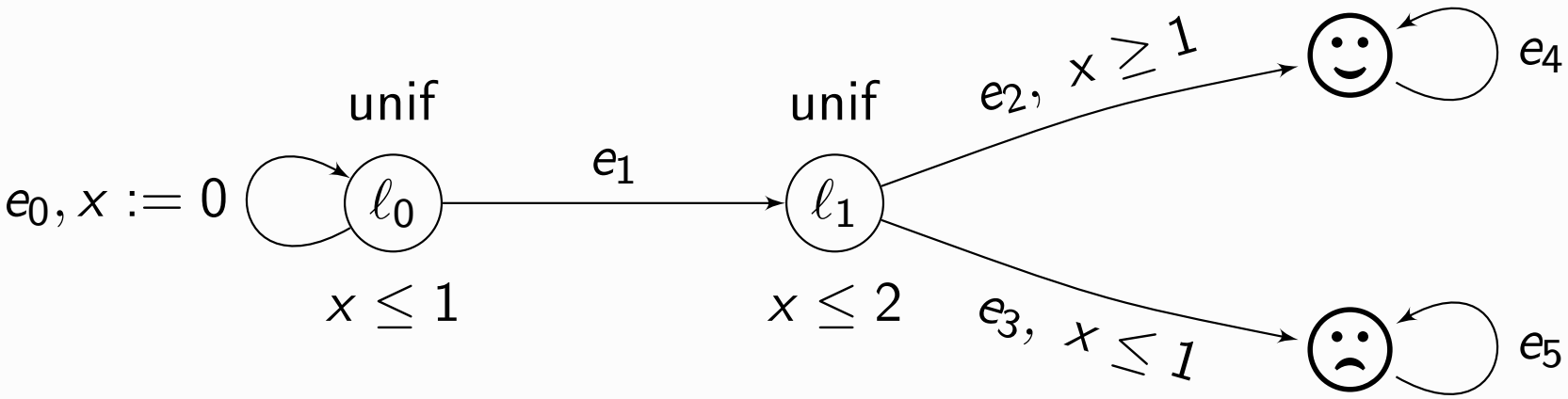
- F is **almost-surely** reachable from s iff

$$\exists \sigma \quad \mathbb{P}^s_\sigma\big((\mathcal{A}, \mu) \models \Diamond F\big) = 1.$$

- F is **limit-surely** reachable from s iff

$$\forall \varepsilon > 0 \; \exists \sigma \quad \mathbb{P}^s_\sigma\big((\mathcal{A}, \mu) \models \Diamond F\big) > 1 - \varepsilon.$$

Almost-sure Vs Limit-sure - continued



- ☺ is not almost-surely reachable from $(\ell_0, 0)$,
- ☺ is limit-surely reachable from $(\ell_0, 0)$.

Remark

On MDPs the limit-sure and almost-sure problems coincide.

Problems considered and results

Probability 1 problem

Input: A DSTA $(\mathcal{A}, \mu)$, a target set $F \subseteq L$ and an initial state $s \in S$.
Question: Is F almost-surely reachable from s?

Value 1 problem

Input: A DSTA $(\mathcal{A}, \mu)$, a target set $F \subseteq L$ and an initial state $s \in S$.
Question: Is F limit-surely reachable from s?

Theorem

The "Probability 1" and "Value 1" are decidable in polynomial time.

Solving the value 1 problem - Key idea

Let $(\mathcal{A}, \mu)$ be a DSTA, we build a **finite MDP** $\mathcal{A}_{\text{cp}}$ such that

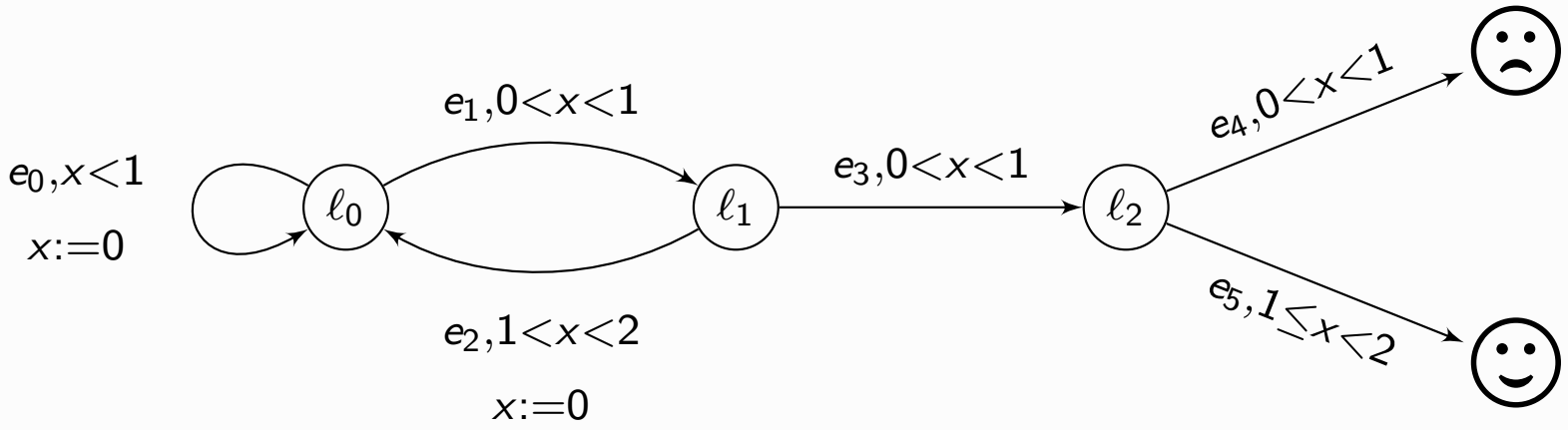
F is **limit-surely** reachable from s_0 in $(\mathcal{A}, \mu)$

if and only if

$\mathcal{F}$ is **almost-surely** reachable from $\tilde{s}_0$ in $\mathcal{A}_{\text{cp}}$.

A new example

All the probability distributions are uniform



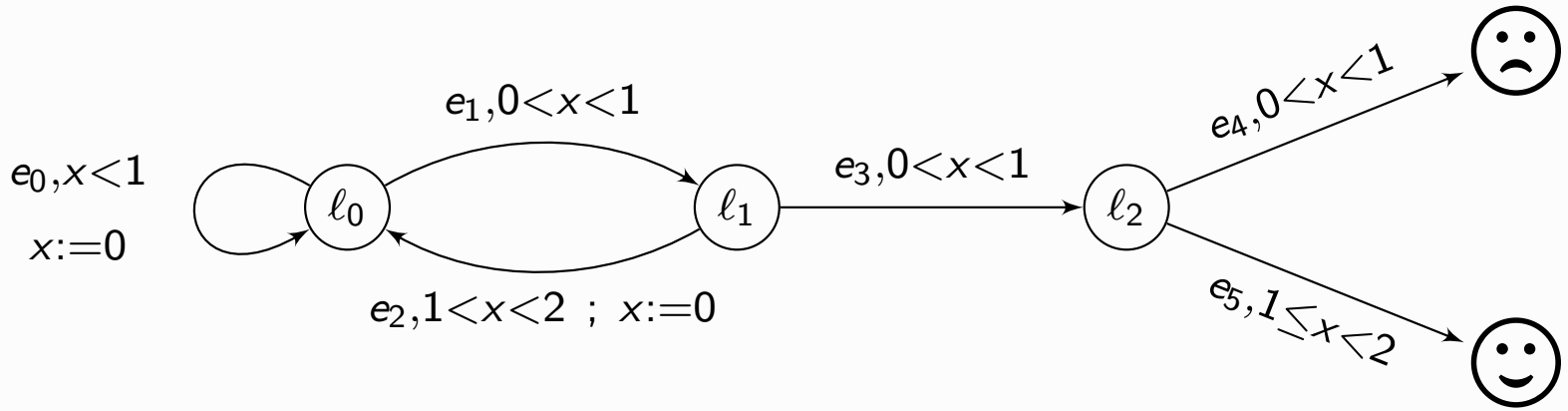
☺ is limit-surely reachable from $(\ell_0, 0)$ with

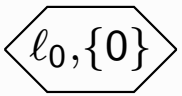
$$\sigma_\varepsilon(\ell_0, \nu) = \begin{cases} e_0 & \text{if } \nu \leq 1-\varepsilon \\ e_1 & \text{if } \nu > 1-\varepsilon \end{cases}$$

Notice that the σ_ε are **not region-uniform** !

Building the limit corner-point region MDP

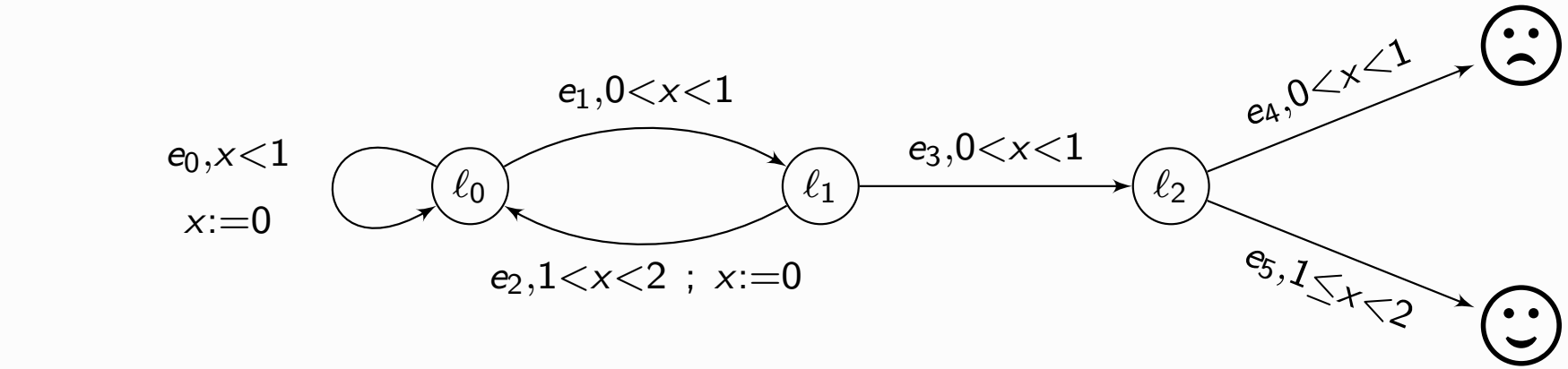
Step 1: The region MDP

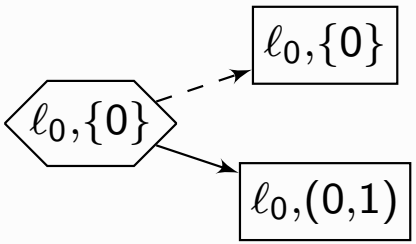




Building the limit corner-point region MDP

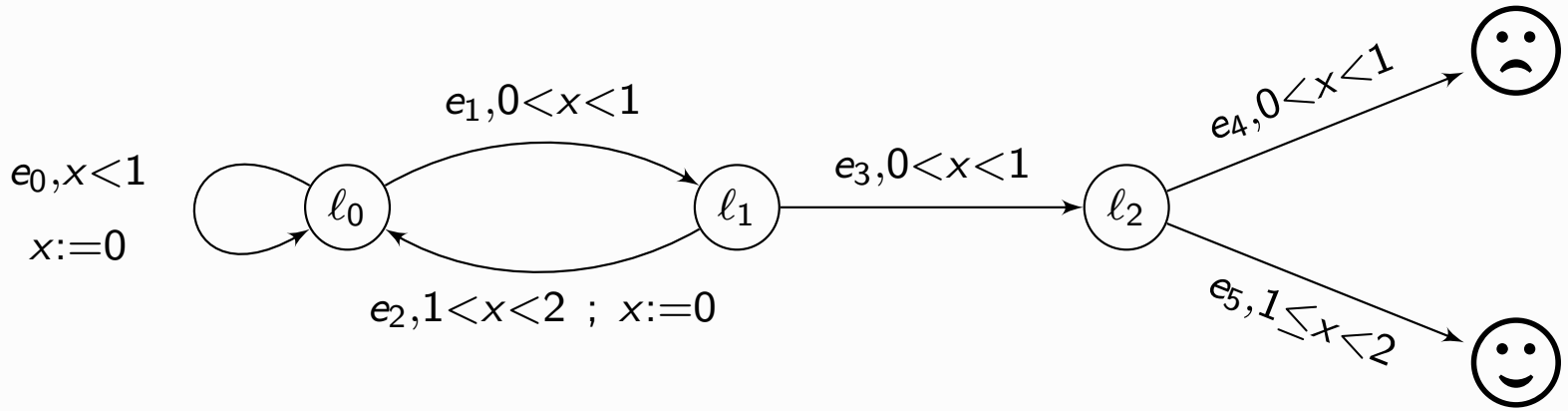
Step 1: The region MDP

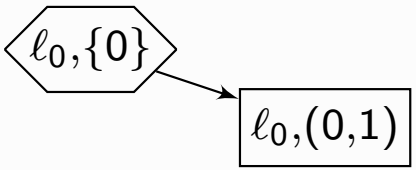




Building the limit corner-point region MDP

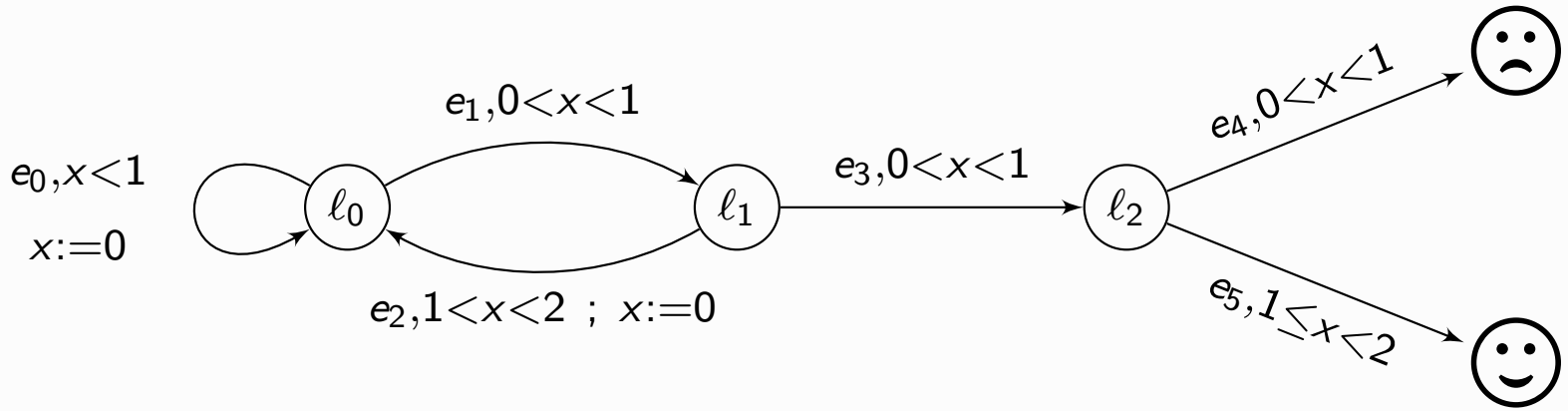
Step 1: The region MDP

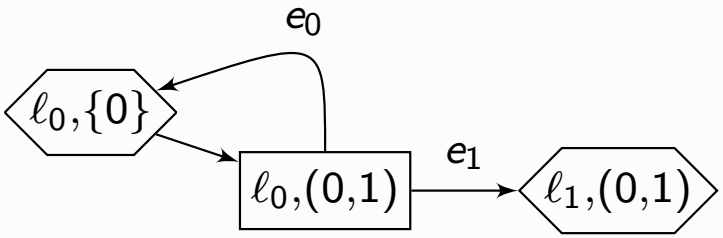




Building the limit corner-point region MDP

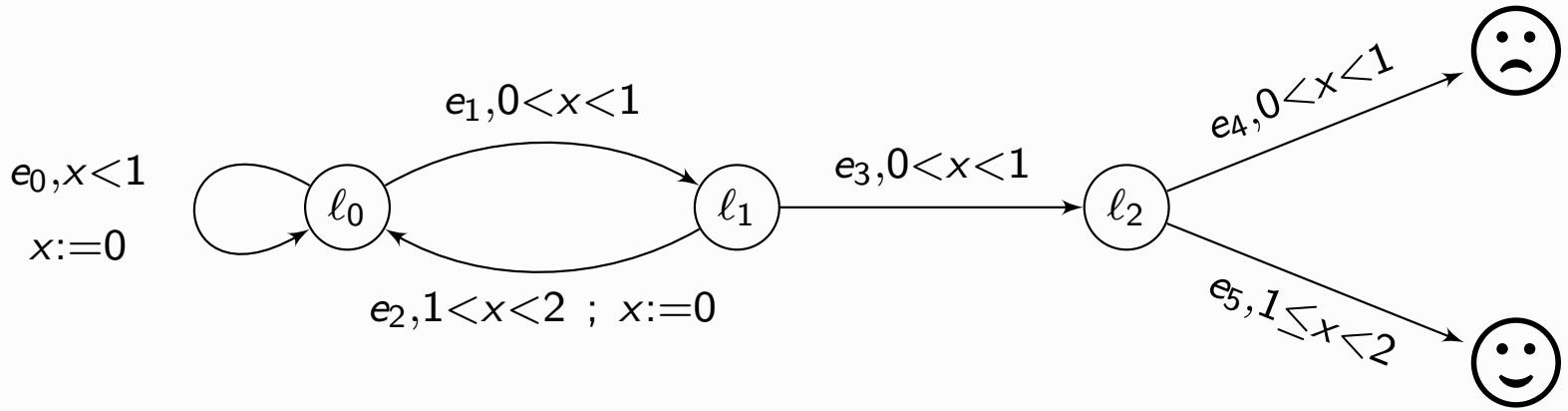
Step 1: The region MDP

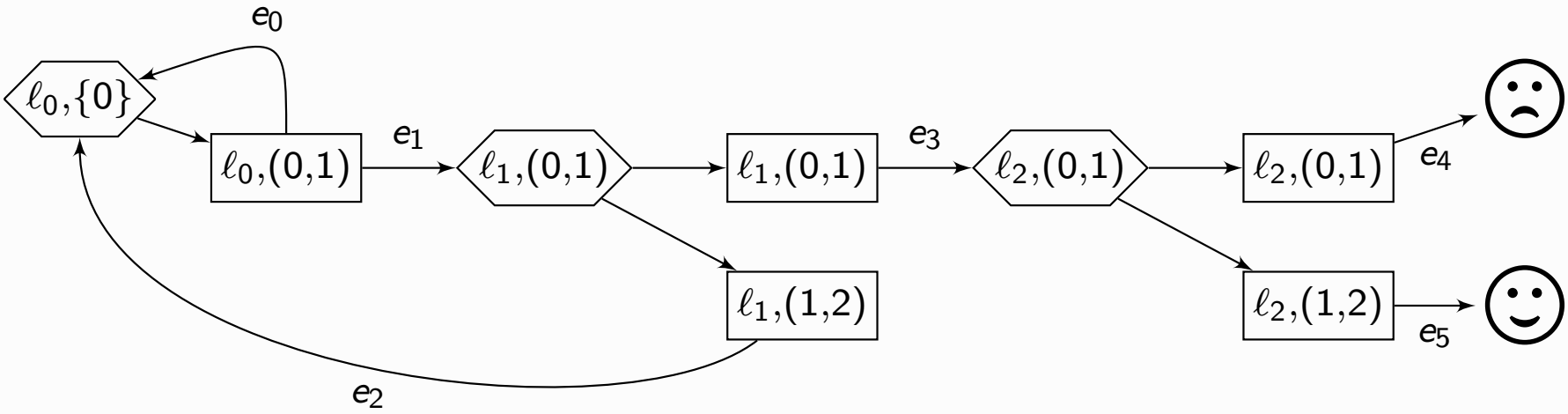




Building the limit corner-point region MDP

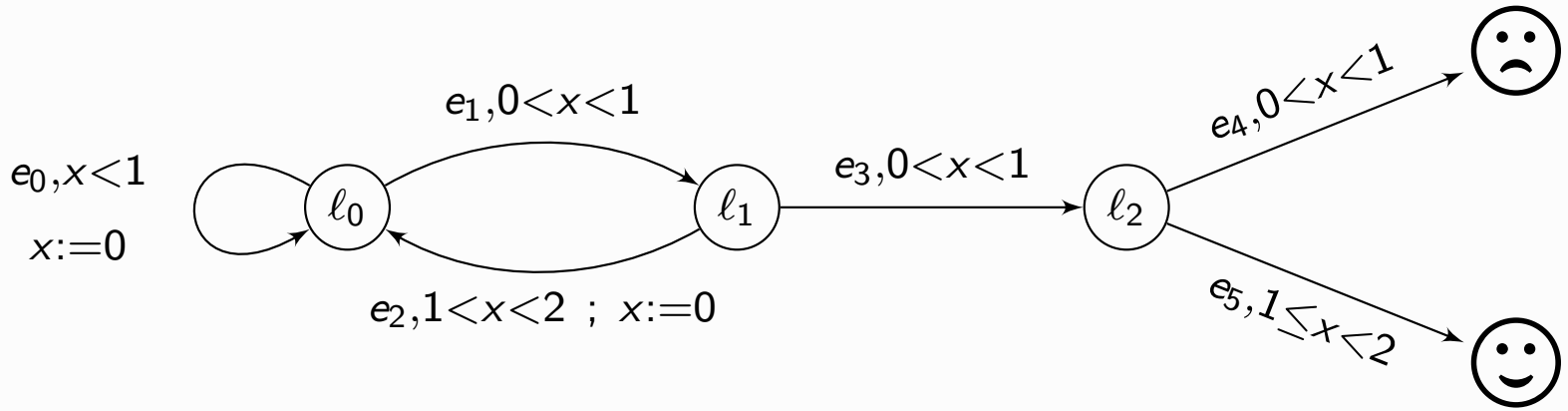
Step 1: The region MDP

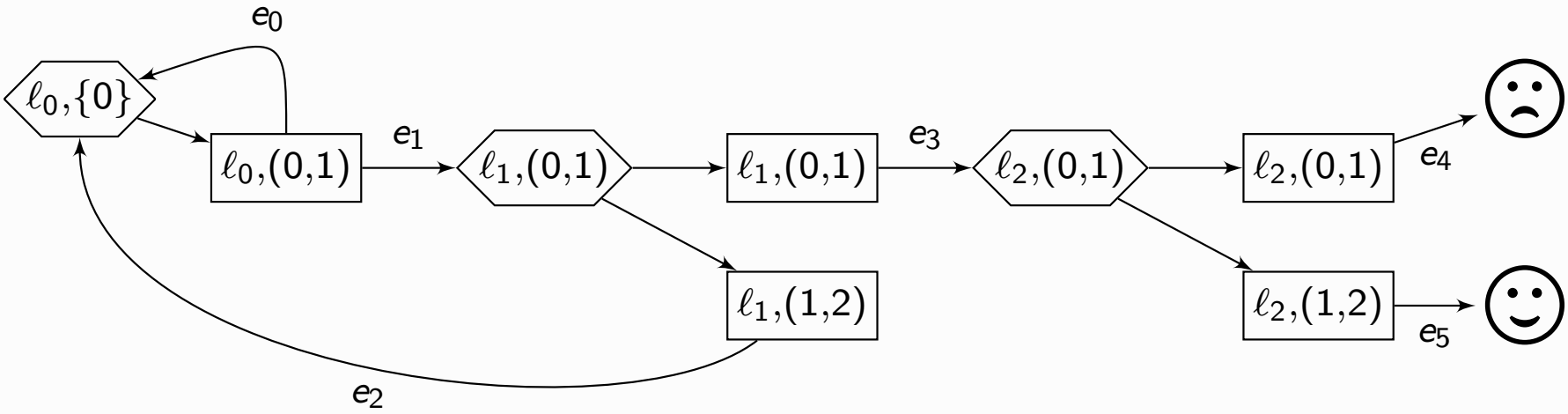




Building the limit corner-point region MDP

Step 1: The region MDP

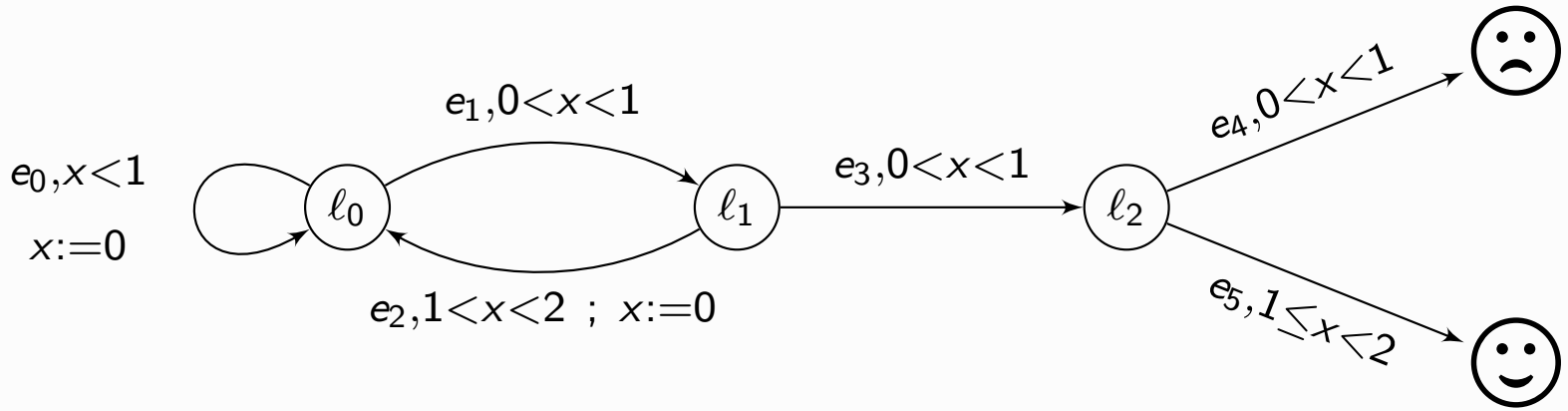




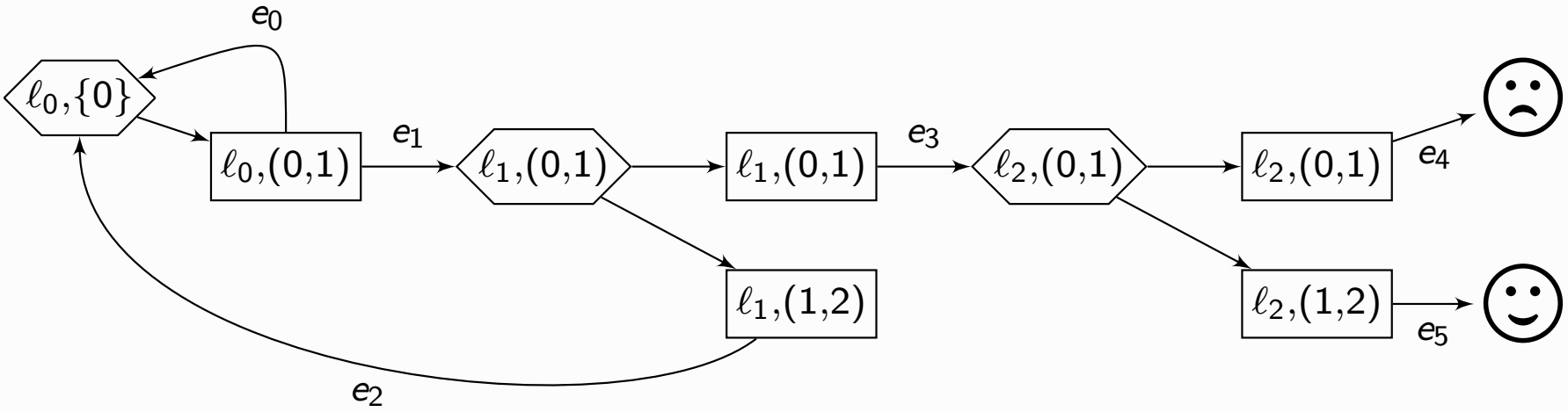
☺ is not almost-surely reachable from $(\ell_0,\{0\})$

Building the limit corner-point region MDP

Step 1: The region MDP



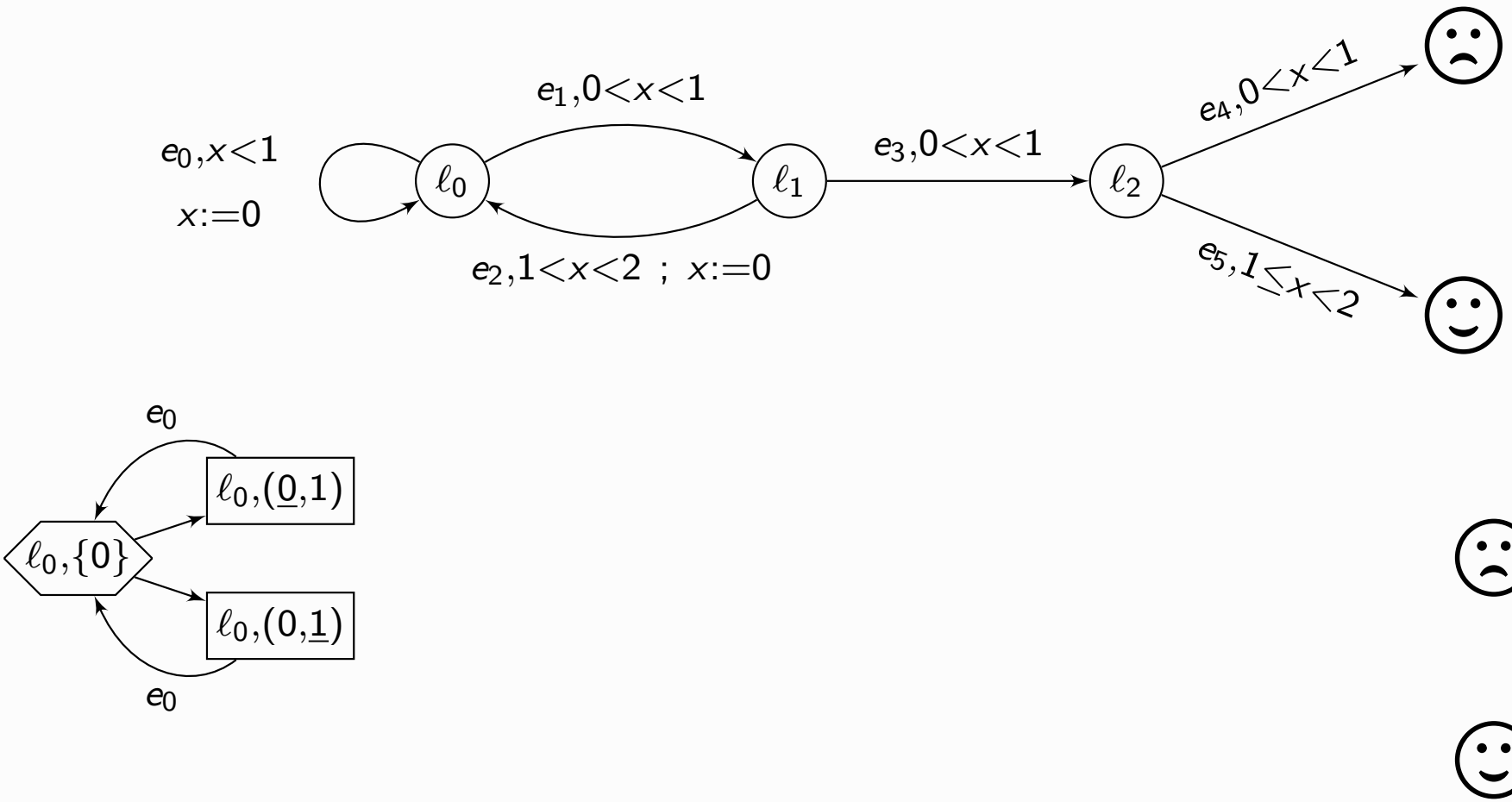
The region MDP is to coarse: ε-optimal strategies are not region uniform.



☺ is not almost-surely reachable from $(\ell_0,\{0\})$

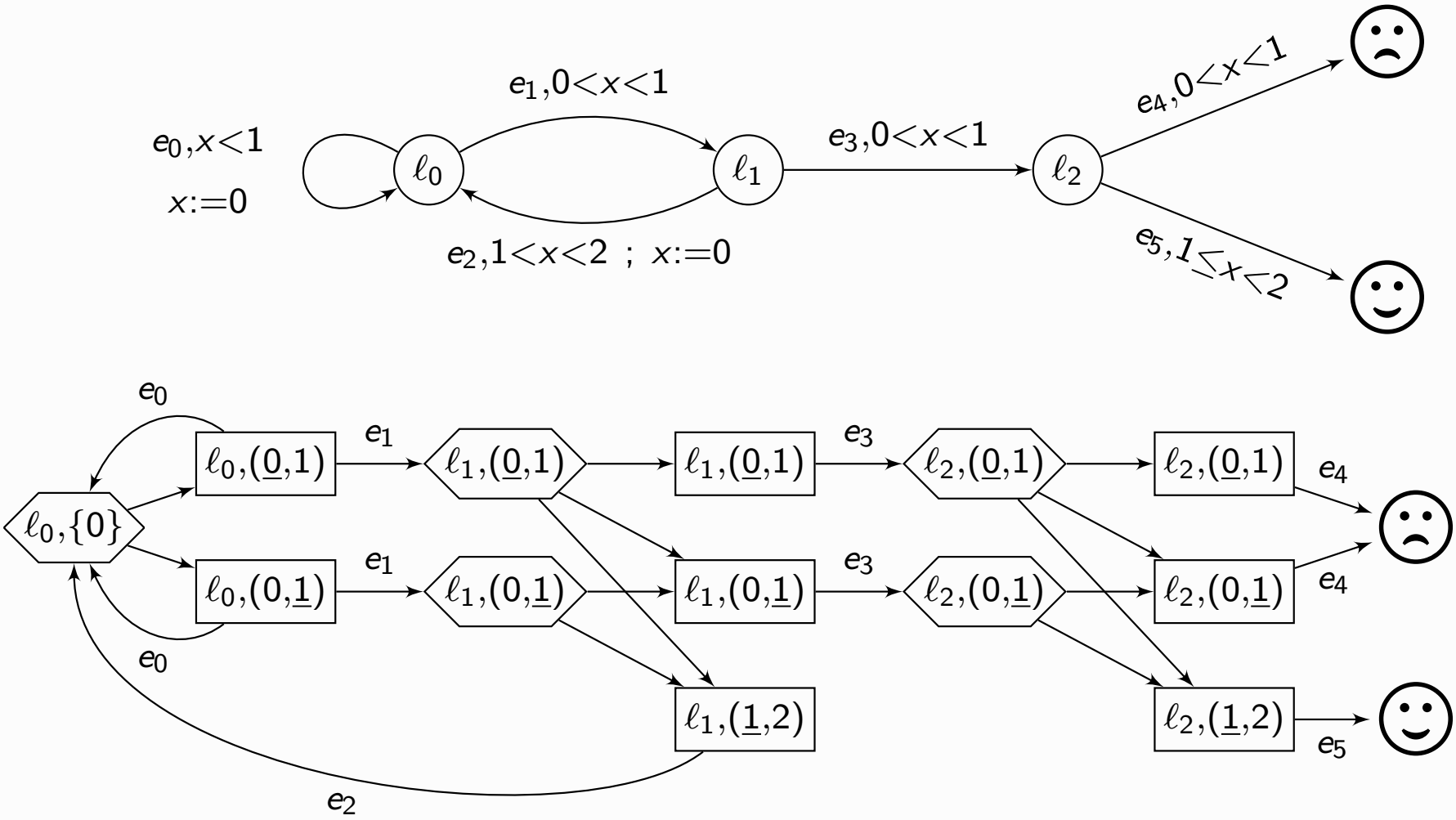
Building the limit corner-point region MDP

Step 2: The corner-point region MDP



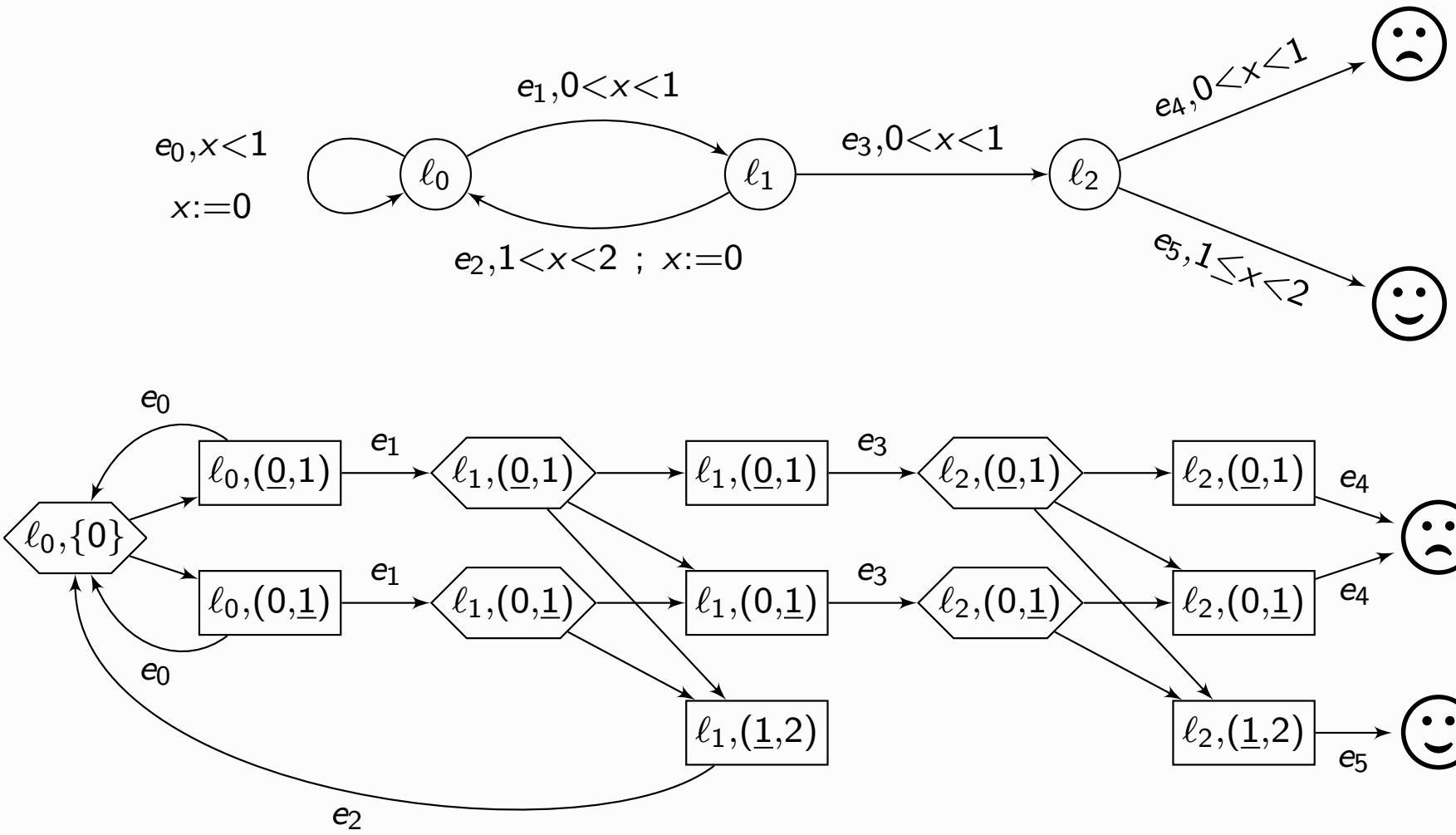
Building the limit corner-point region MDP

Step 2: The corner-point region MDP



Building the limit corner-point region MDP

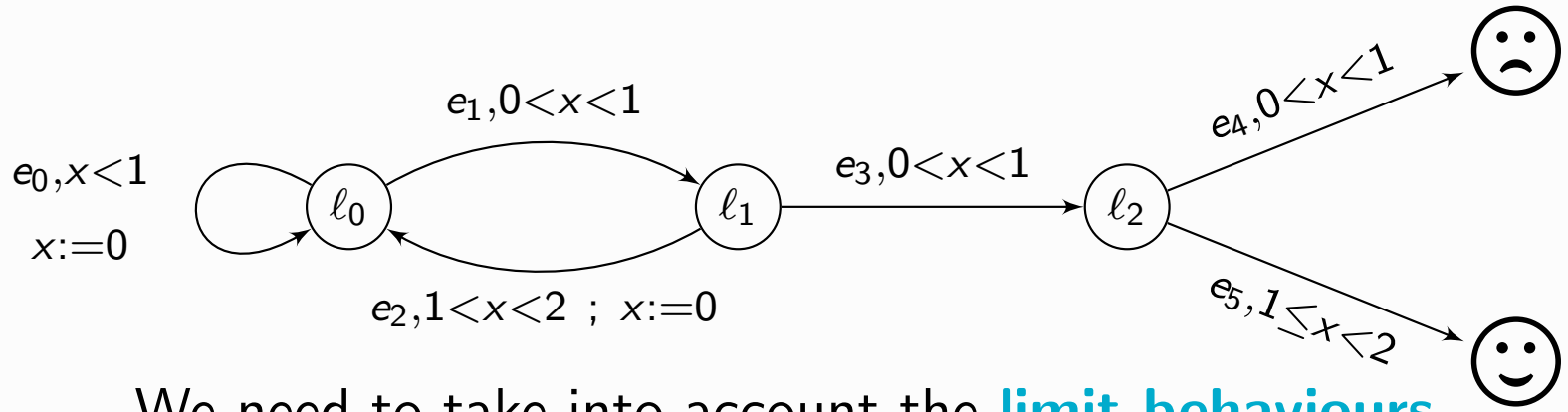
Step 2: The corner-point region MDP



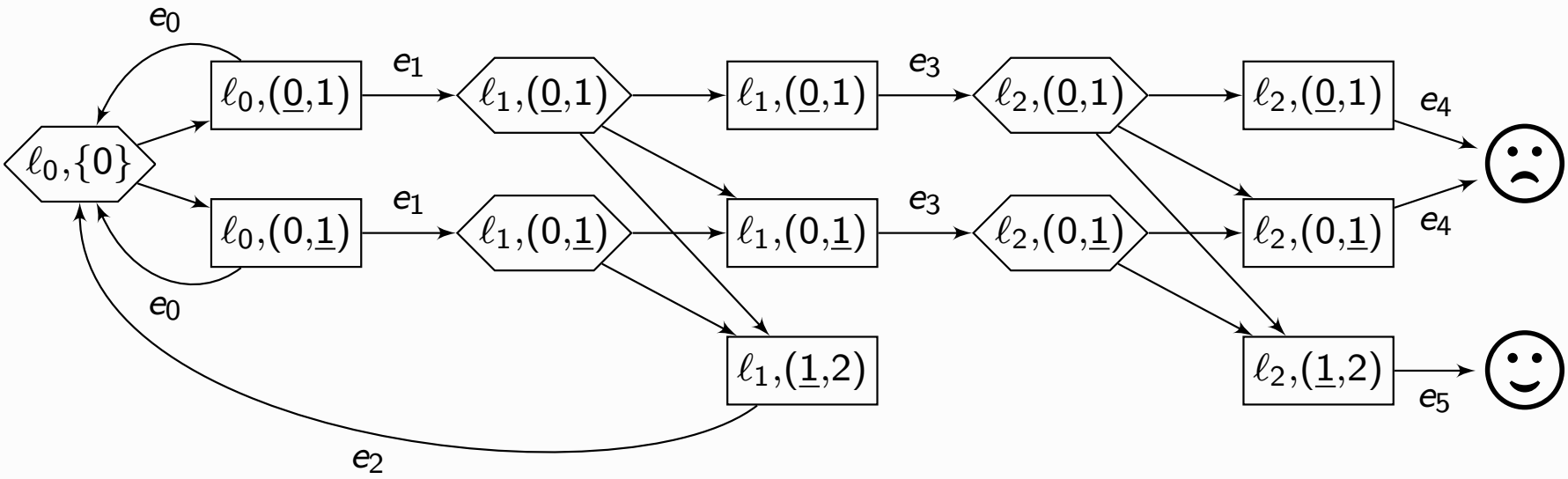
☺ is not almost-surely reachable from $(\ell_0,\{0\})$

Building the limit corner-point region MDP

Step 2: The corner-point region MDP



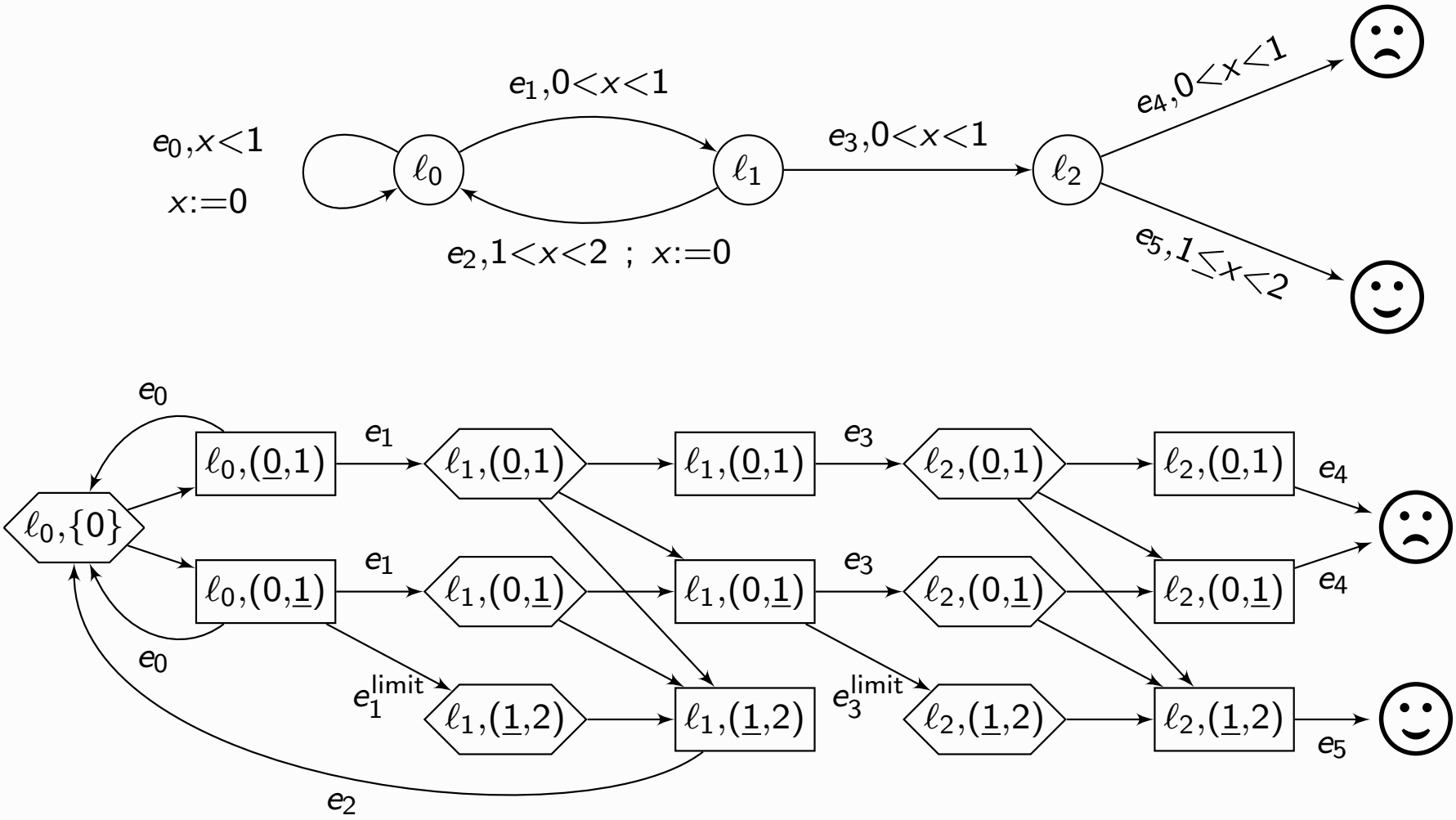
We need to take into account the **limit behaviours**.



☺ is not almost-surely reachable from $(\ell_0,\{0\})$

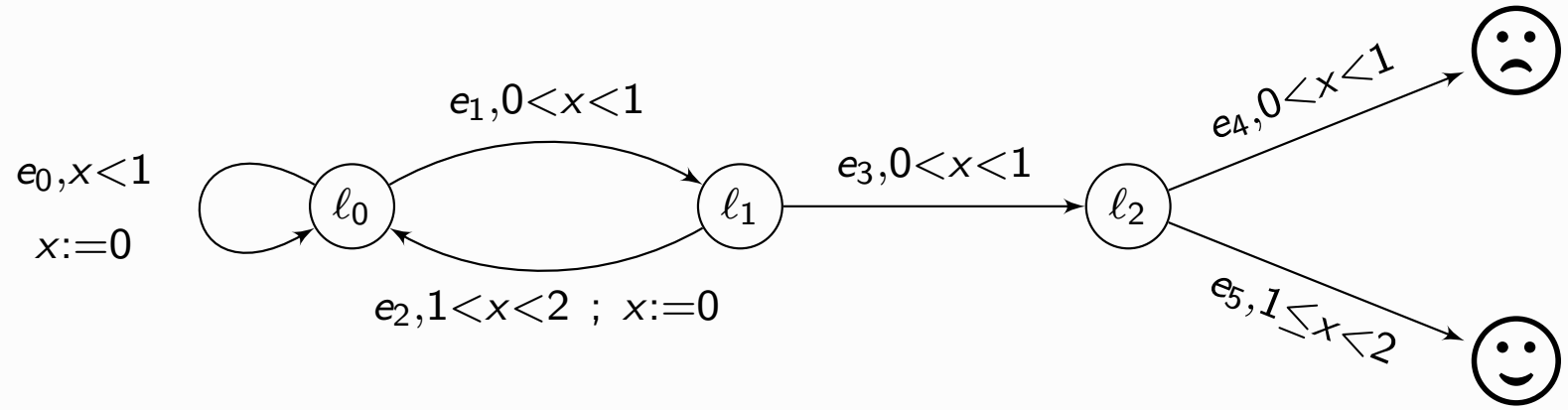
Building the limit corner-point region MDP

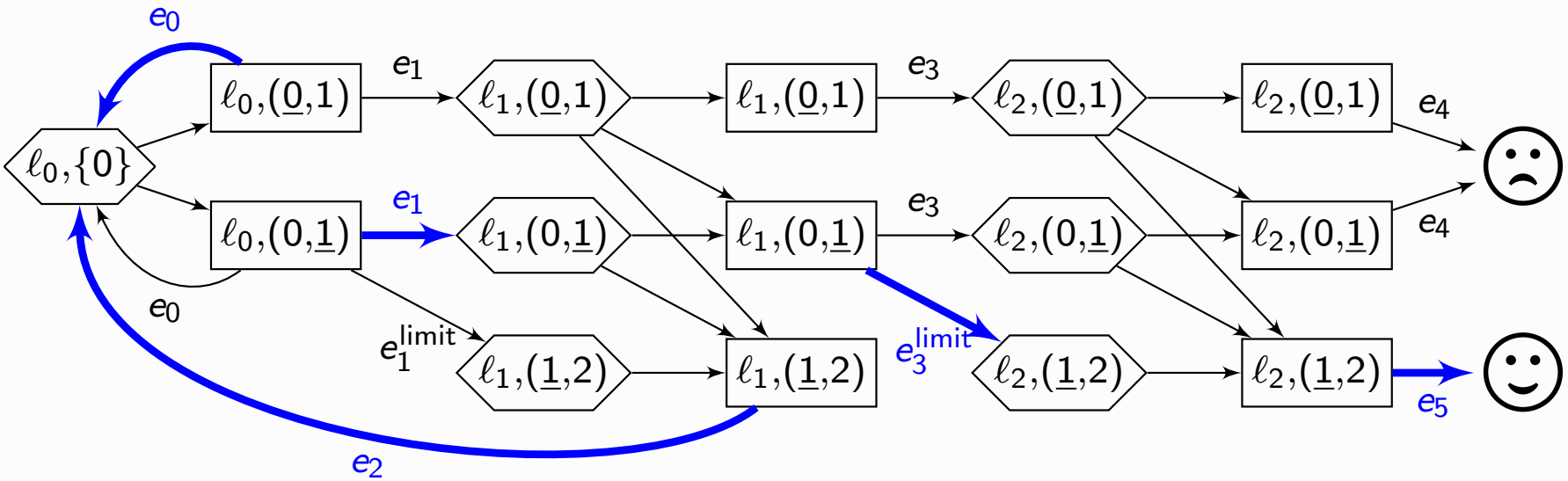
Step 3: The limit corner-point region MDP



Building the limit corner-point region MDP

Step 3: The limit corner-point region MDP





☺ is almost-surely reachable from $(\ell_0,\{0\})$

The limit corner-point MDP

When do we add limit-edges ?

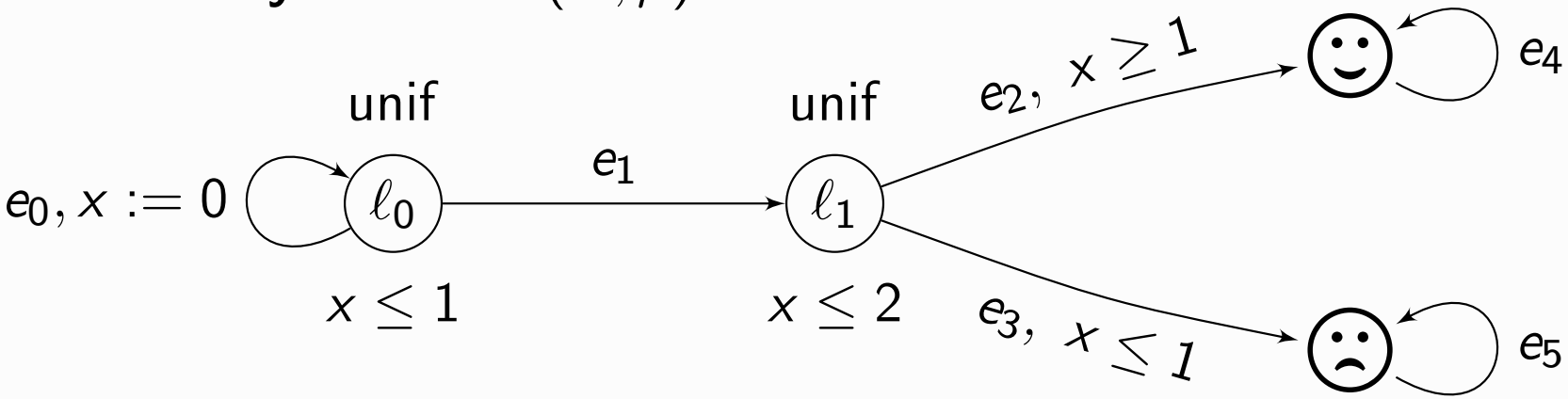
$$\mathcal{A} = (L, \ell_0, E, \mathcal{I}, \mu) \rightsquigarrow \mathcal{A}_{\text{cp}} = (\mathcal{S}, \mathbf{s}_0, \text{Act}, \Delta)$$

- $\mathcal{S} = \{[\ell, \mathbf{r}] \mid \ell \in L,\ \mathbf{r} \in \mathbf{R}\} \cup \{\langle \ell, \mathbf{r}\rangle \mid \ell \in L,\ \mathbf{r} \in \mathbf{R}\}$, where $\mathbf{R}$ is the set of **pointed region**, i.e. of the form $\{a\}$, $(\underline{a}, b)$ or $(a, \underline{b})$.
- $\text{Act} = E \cup E^{\text{limit}}$, where E^{limit} is a copy of E;
- Δ consists of the following transitions:
  - $\langle \ell, \mathbf{r}\rangle \xrightarrow{\tau} [\ell, \mathbf{r}']$ if $\mathbf{r} \leq \mathbf{r}'$ (not negligible), the probabilities are uniform;
  - $[\ell, \mathbf{r}] \xrightarrow{e} \langle \ell', \{0\}\rangle$ if $e = (\ell, g, \{x\}, \ell') \in E$, and $\mathbf{r} \models g$;
  - $[\ell, \mathbf{r}] \xrightarrow{e} \langle \ell', \mathbf{r}\rangle$ if $e = (\ell, g, \emptyset, \ell') \in E$, and $\mathbf{r} \models g$;
  - **$[\ell, \mathbf{r}] \xrightarrow{e^{\text{limit}}} \langle \ell', \mathbf{r}'\rangle$ if $\mathbf{r} \in \mathbf{R}_{\text{right}}$, $e = (\ell, g, \emptyset, \ell') \in E$, $\mathbf{r} \models g$, $\mathbf{r}'$ is the immediate open successor of $\mathbf{r}$, and $\mathbf{r}' \models \mathcal{I}(\ell')$.**

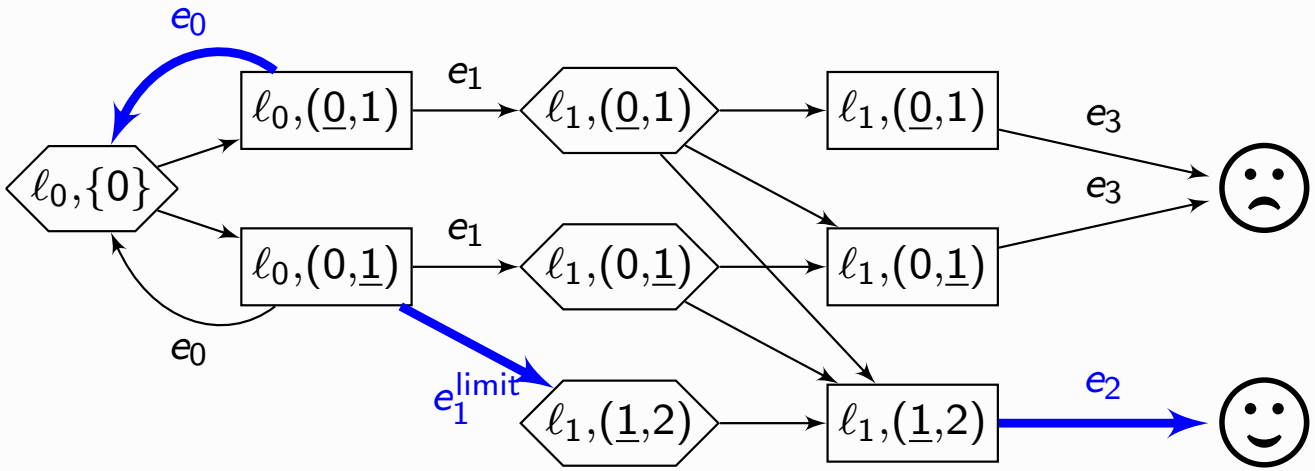
Do we give too much power to the non-det. player ?

Back to the first example

F is **limit-surely** reach. in $(\mathcal{A}, \mu)$



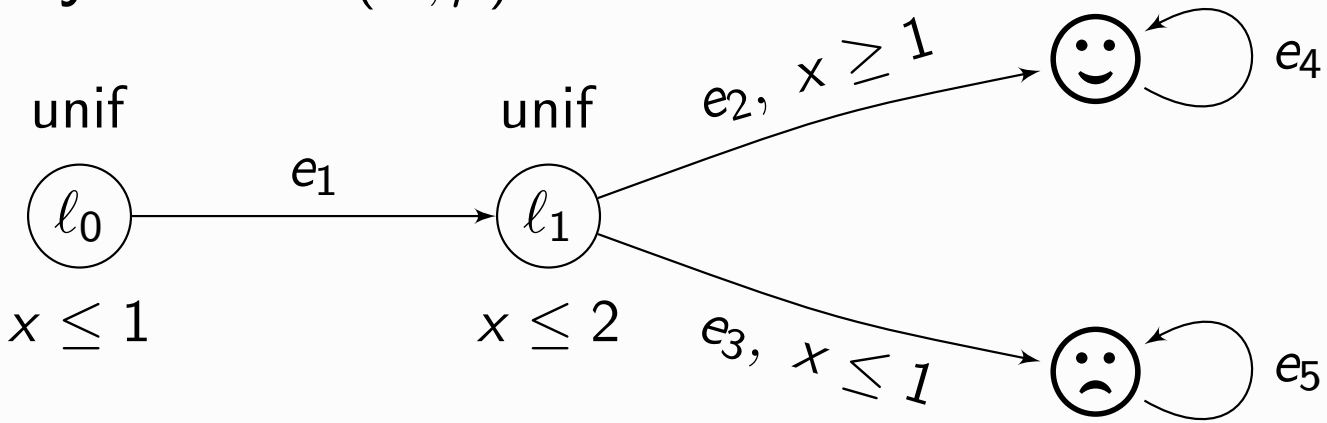
$\mathcal{F}$ is **almost-surely** reach. in $\mathcal{A}_{\mathsf{cp}}$.



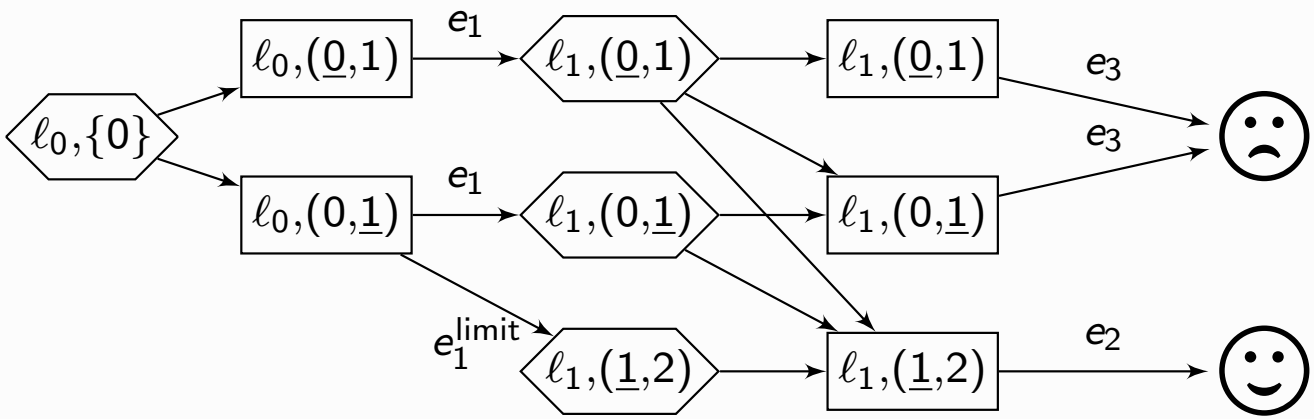
Do we give too much power to the non-det. player ?

A variation of the first example

F is **not** **limit-surely** reach. in $(\mathcal{A}, \mu)$



$\mathcal{F}$ is **not** **almost-surely** reach. in $\mathcal{A}_{\text{cp}}$.



Proof of the main result (I)

Proposition

Let $(\mathcal{A}, \mu)$ be a DSTA and $\mathcal{A}_{\text{cp}}$ its limit corner-point MDP.
Let s_0 be a state $\mathcal{A}$, $F \subseteq L$, and $\tilde{s}_0$, $\mathcal{F}$ their counterpart in $\mathcal{A}_{\text{cp}}$.

If F is **limit-surely** reachable from s_0 in $(\mathcal{A}, \mu)$,
then $\mathcal{F}$ is **almost-surely** reachable from $\tilde{s}_0$ in $\mathcal{A}_{\text{cp}}$.

Proof of the main result (II)

Proposition

Let $(\mathcal{A}, \mu)$ be a DSTA and $\mathcal{A}_{\text{cp}}$ its limit corner-point MDP.
Let s_0 be a state $\mathcal{A}$, $F \subseteq L$, and $\tilde{s}_0$, $\mathcal{F}$ their counterpart in $\mathcal{A}_{\text{cp}}$.

If $\mathcal{F}$ is **almost-surely** reachable from $\tilde{s}_0$ in $\mathcal{A}_{\text{cp}}$,
then F is **limit-surely** reachable from s_0 in $(\mathcal{A}, \mu)$.

Classical algorithm on MDPs

Computing the set of states reaching $\mathcal{F}$ almost-surely

- **Init:** $\mathcal{W} := \mathcal{S}_\Box$, for every $\mathbf{s} \in \mathcal{S}_\Box$, $\mathsf{Safe}(\mathbf{s}) := \mathsf{Enabled}(\mathbf{s})$.
- Perform steps 1 and 2 until convergence.

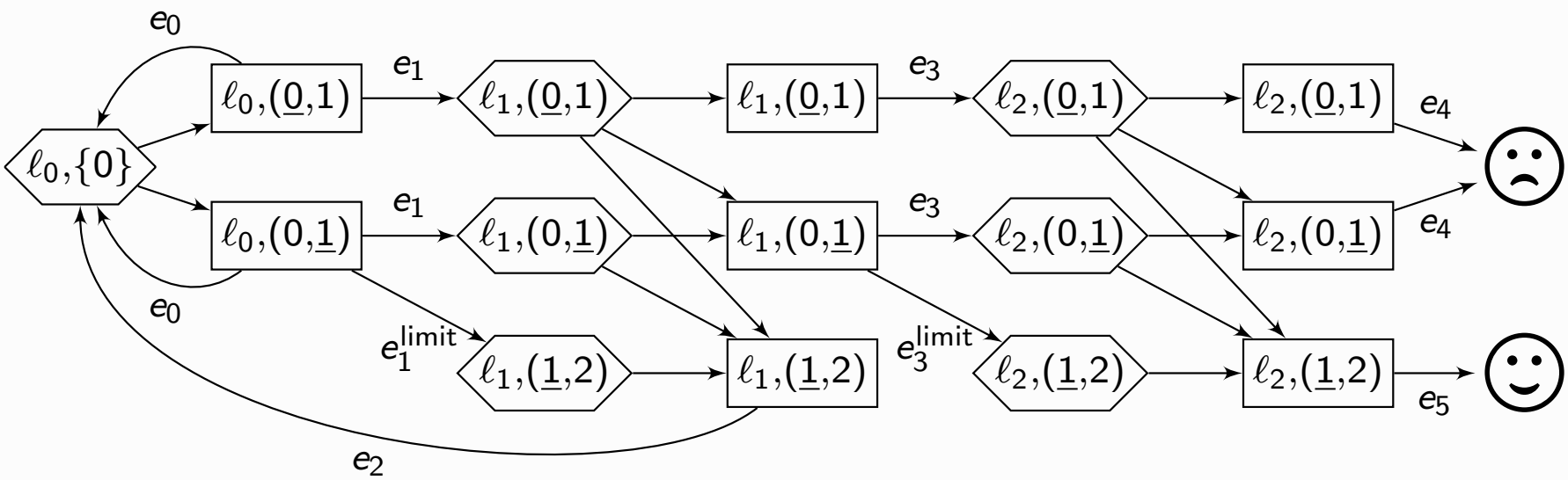
  Step 1: $\mathcal{W} := \mathcal{W} \setminus \{[\ell, \mathbf{r}] \mid [\ell, \mathbf{r}] \not\models \mathcal{W} \exists \mathsf{U} \mathcal{F}\}$

  Step 2:
  - $\mathsf{Safe}([\ell, \mathbf{r}]) = \mathsf{Safe}([\ell, \mathbf{r}]) \setminus \{e \mid \exists \mathbf{r}'' \text{ s.t. } [\ell, \mathbf{r}] \xrightarrow{e} \langle \ell', \mathbf{r}' \rangle \to [\ell', \mathbf{r}''] \notin \mathcal{W}\}$
  - $\mathcal{W} := \mathcal{W} \setminus \{[\ell, \mathbf{r}] \mid \mathsf{Safe}([\ell, \mathbf{r}]) = \emptyset\}$.
- **Return** $(\mathcal{W}, \mathsf{Safe})$.

$\mathcal{W}$ is the set of the winning states, $\mathsf{Safe}(\mathbf{w})$ is the set of safe actions.

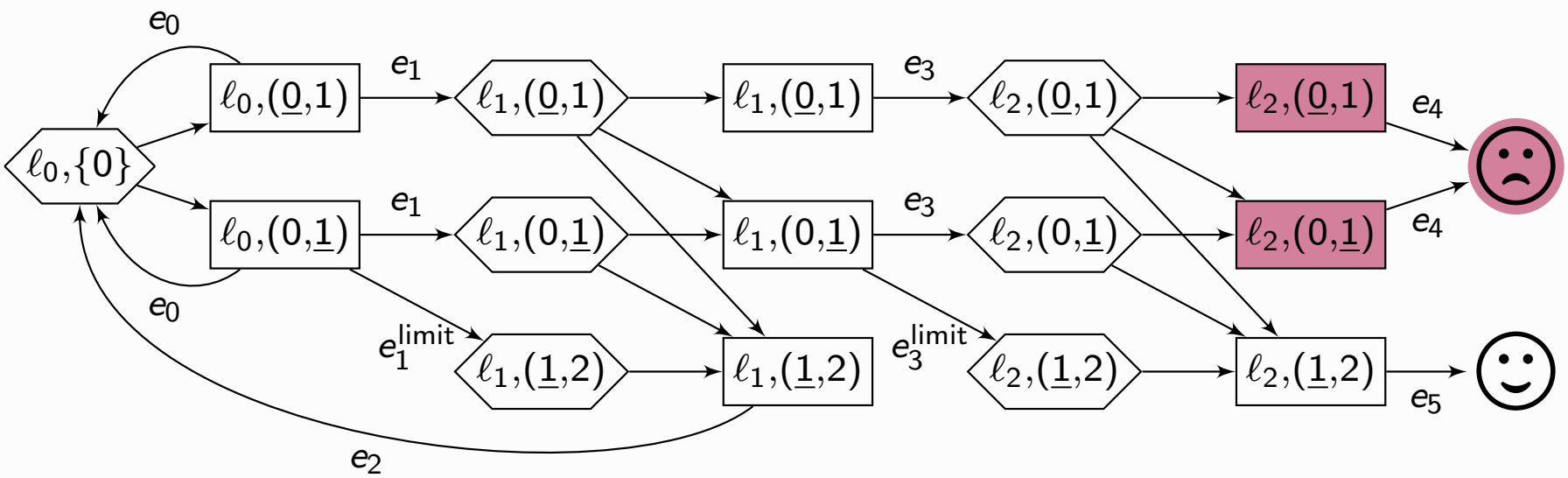
Back to our example

Applying the MDPs algorithm



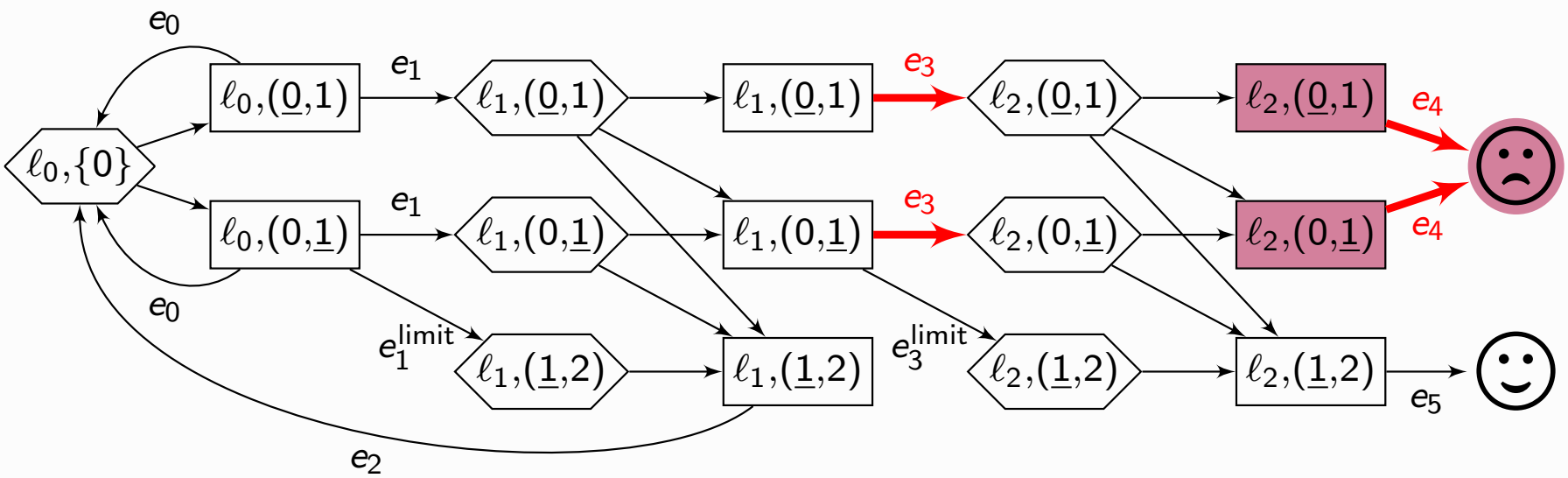
Back to our example

Applying the MDPs algorithm



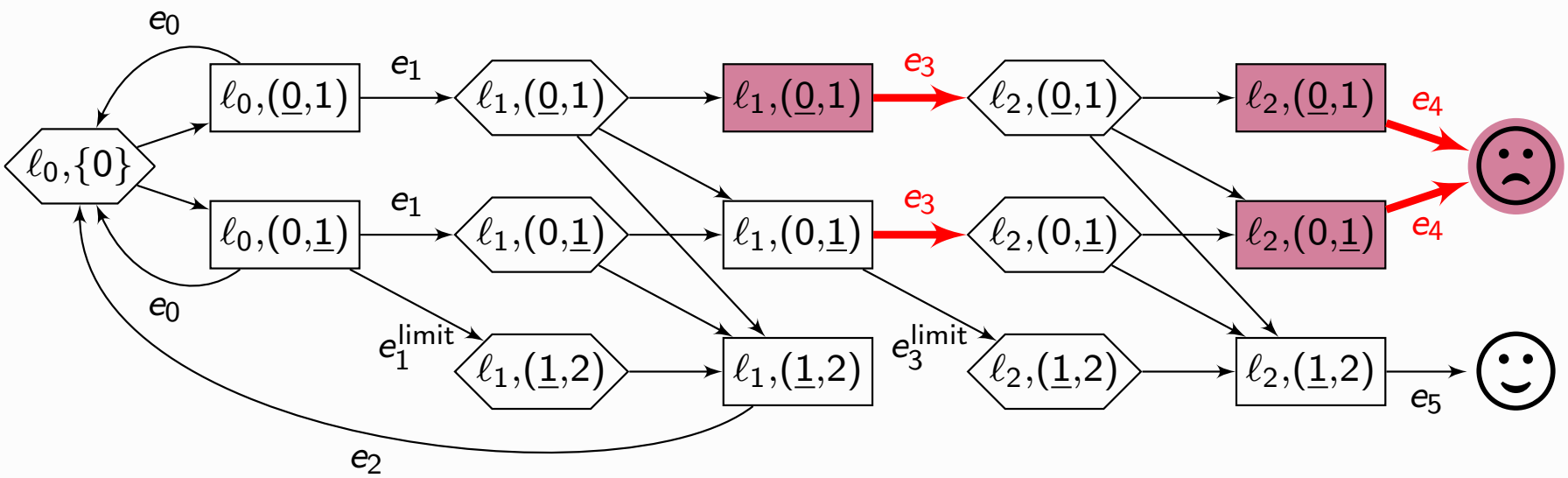
Back to our example

Applying the MDPs algorithm



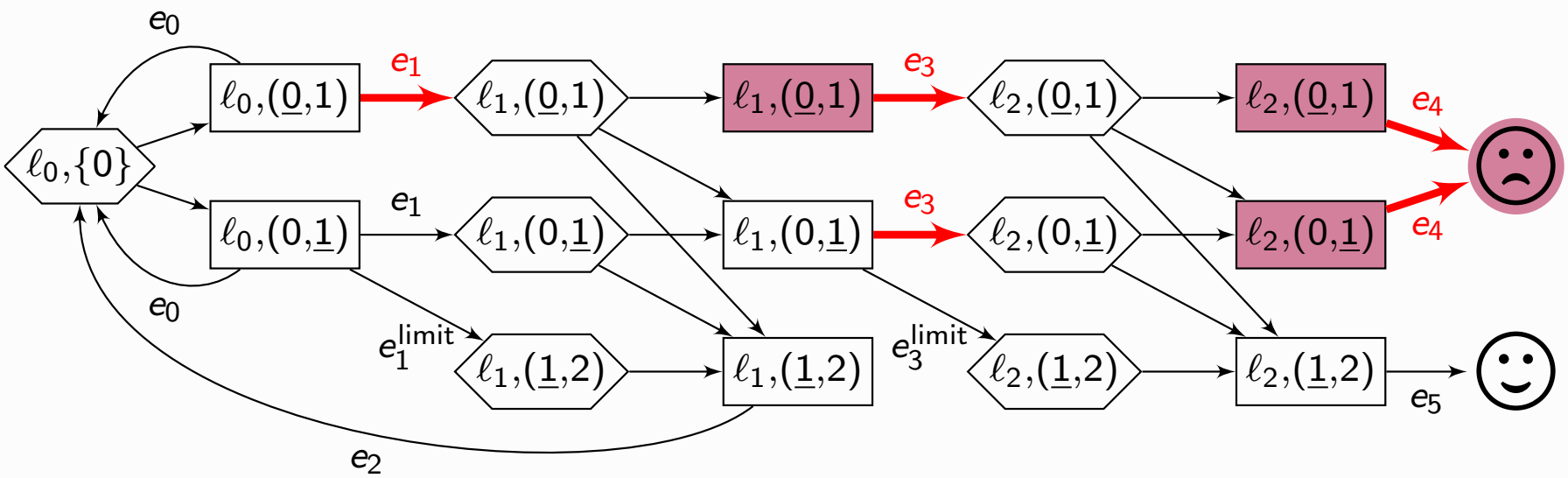
Back to our example

Applying the MDPs algorithm



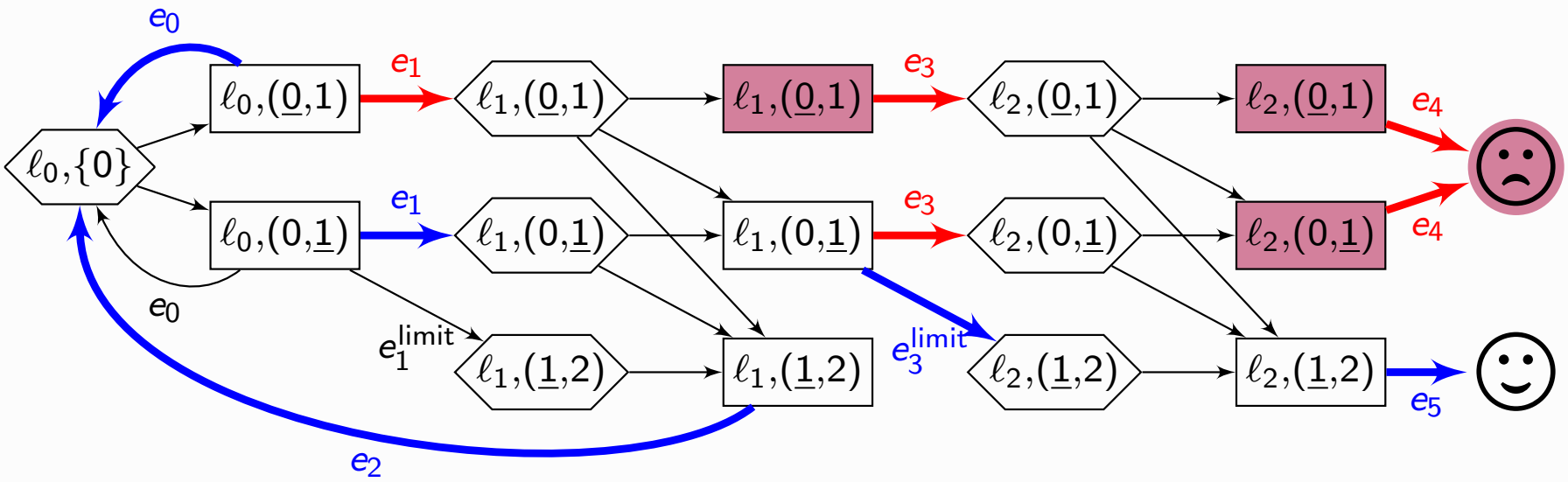
Back to our example

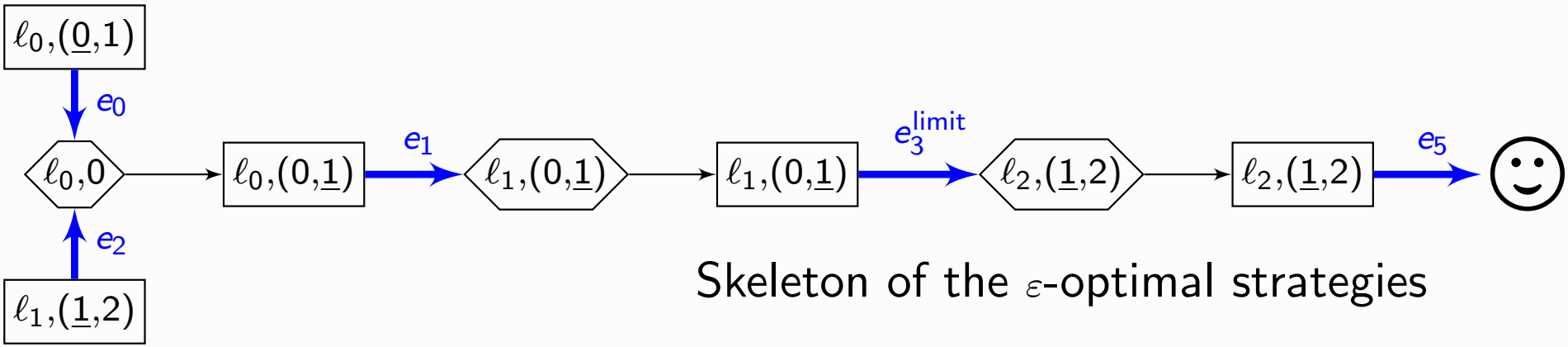
Applying the MDPs algorithm



Back to our example

Applying the MDPs algorithm

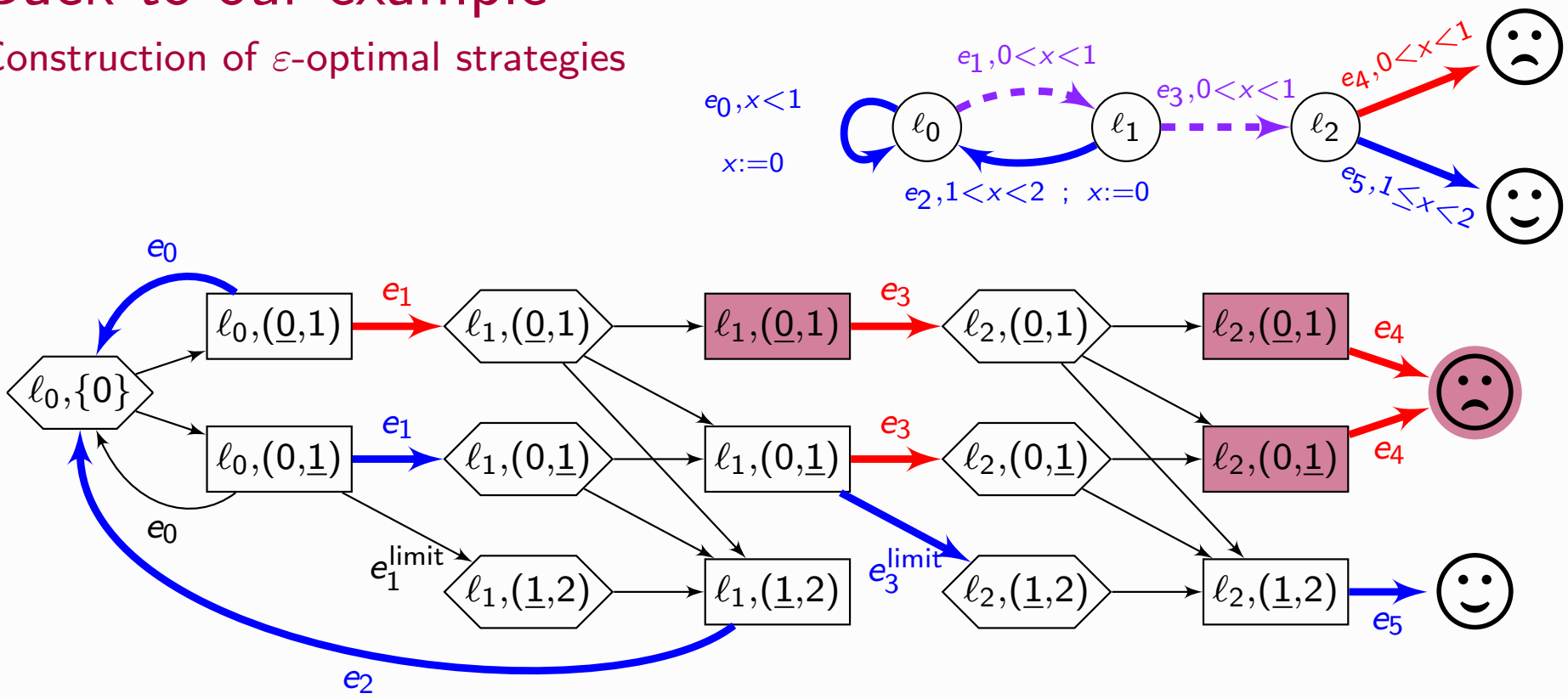




Skeleton of the ε-optimal strategies

Back to our example

Construction of ε-optimal strategies

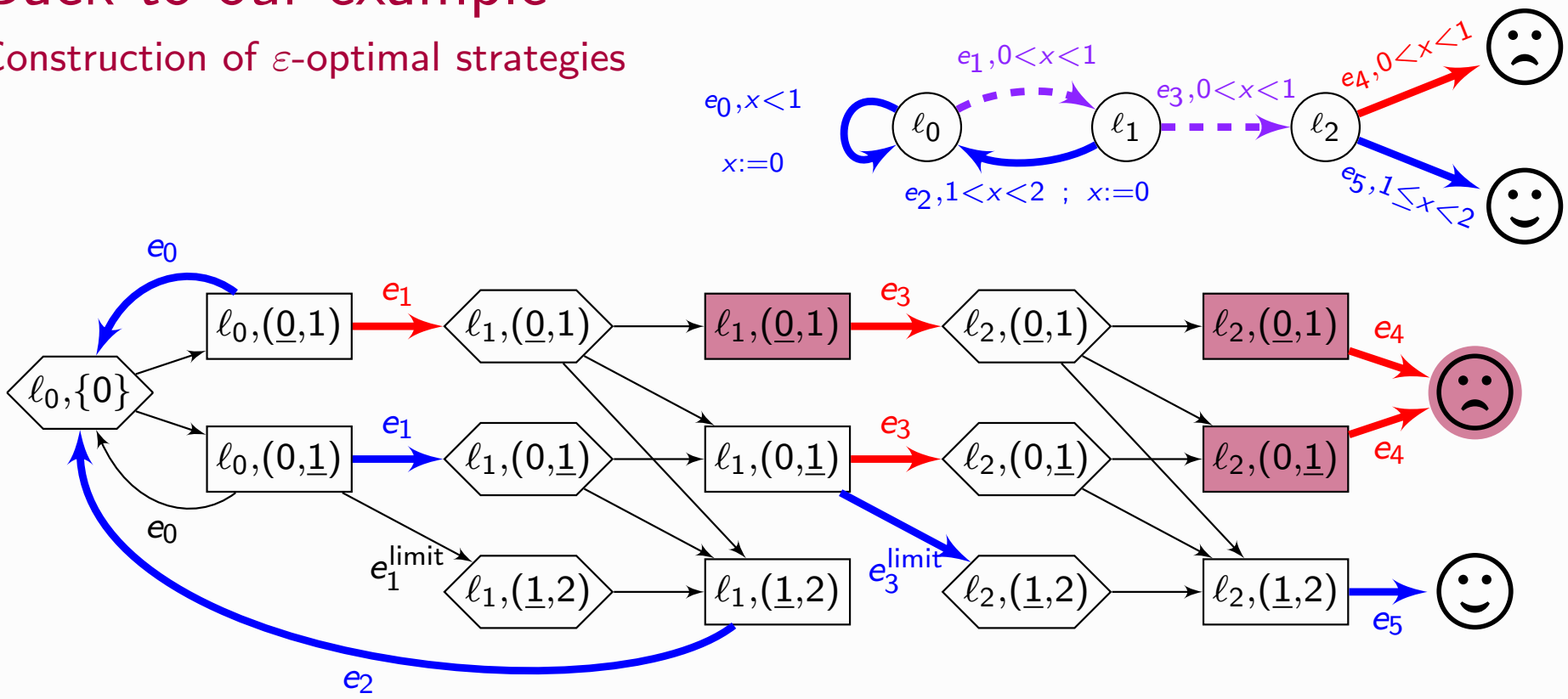


Roughly speaking, in the DSTA:

- Playing edges corresponding to **non-limit edges** is **safe**.
- Playing edges corresponding to **limit edges** is **risky**.

Back to our example

Construction of ε-optimal strategies

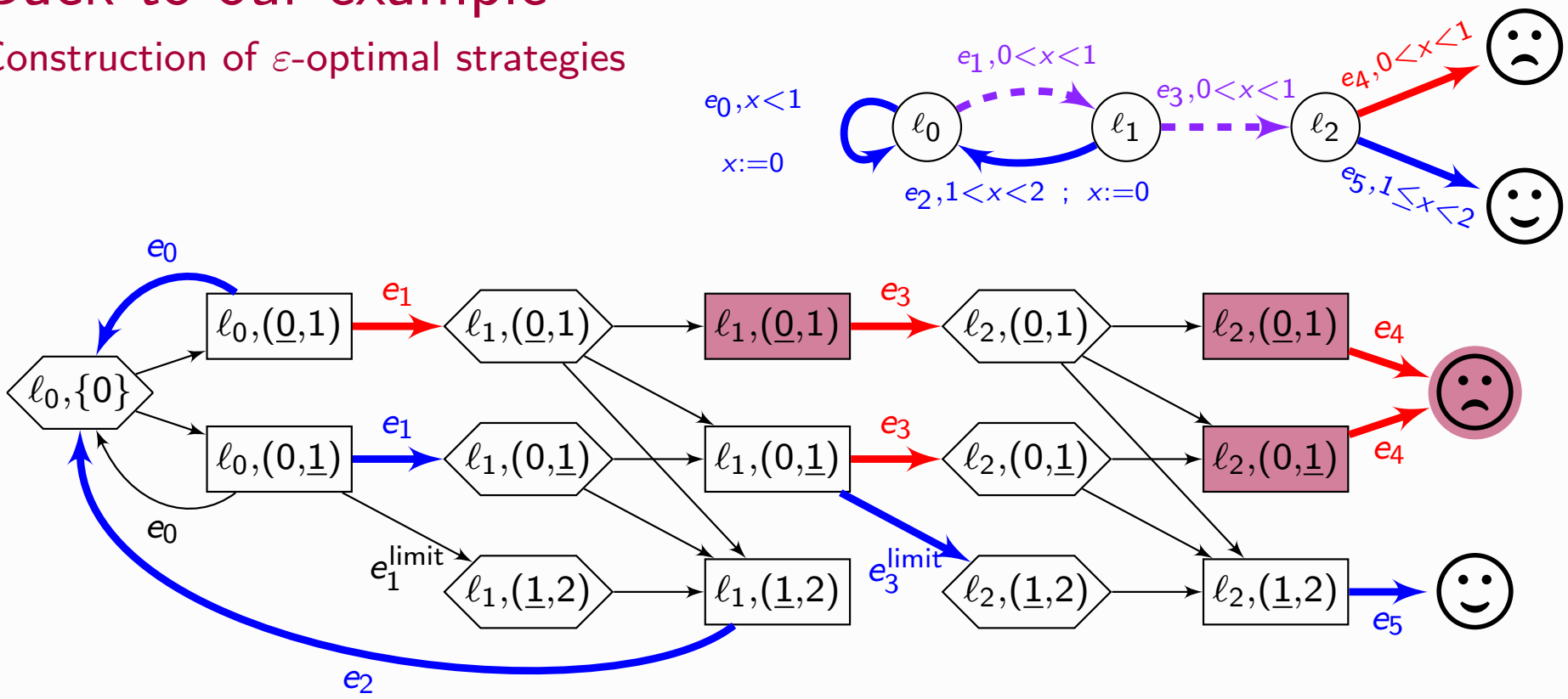


For every $\varepsilon > 0$, there exists $T : L \times R \to \mathbb{R}_{\geq 0}$ and a strategy σ_T

- For every $\mathbf{s} \in \tilde{\mathcal{W}}_T$, $\mathbb{P}^{\mathcal{A}}_{\sigma_T}(\mathbf{s} \models \Diamond(F \cup S_T^{\text{right}})) = 1$
- if $\sigma_T(s) \in E^{\text{limit}}$ then $\mathbb{P}^s_{\sigma_T}(\bigcirc\tilde{\mathcal{W}}_T) \geq 1 - \varepsilon$, else $\mathbb{P}^s_{\sigma_T}(\bigcirc\tilde{\mathcal{W}}_T) = 1$.

Back to our example

Construction of ε-optimal strategies

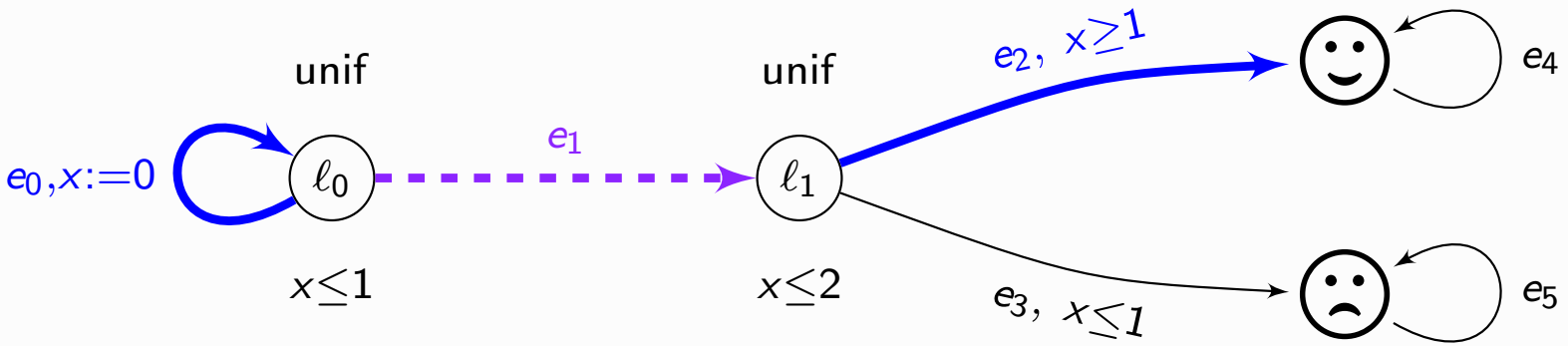


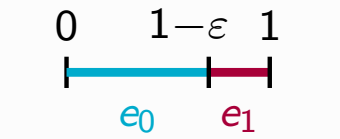
For every $\varepsilon > 0$, there exists $T : L \times R \to \mathbb{R}_{\geq 0}$ and a strategy σ_T

- For every $\mathbf{s} \in \tilde{\mathcal{W}}_T$, $\mathbb{P}^{\mathcal{A}}_{\sigma_T}(\mathbf{s} \models \Diamond F) \geq 1 - \varepsilon$.

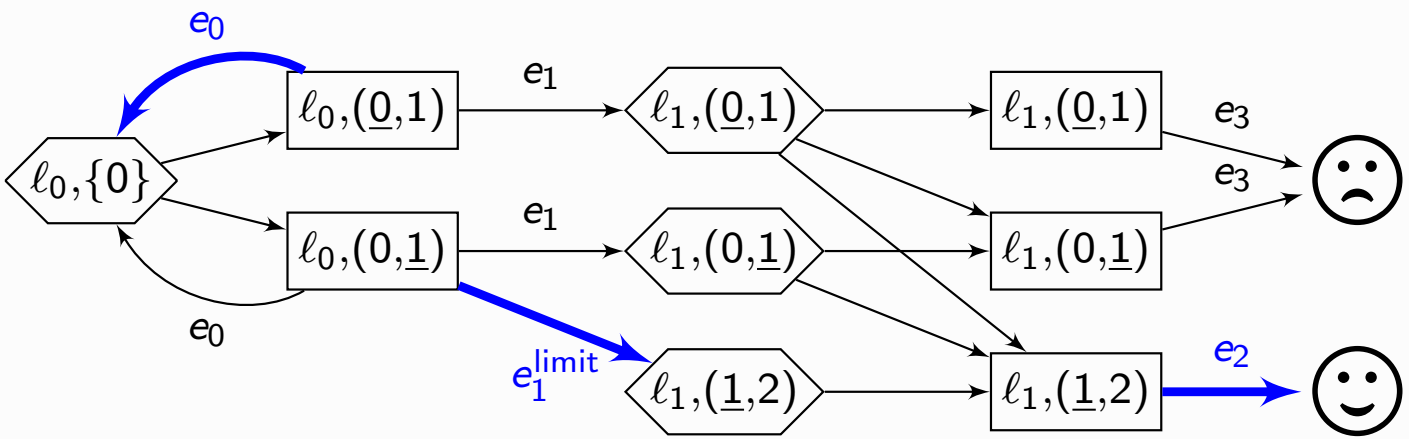
About the construction of T

A simple case





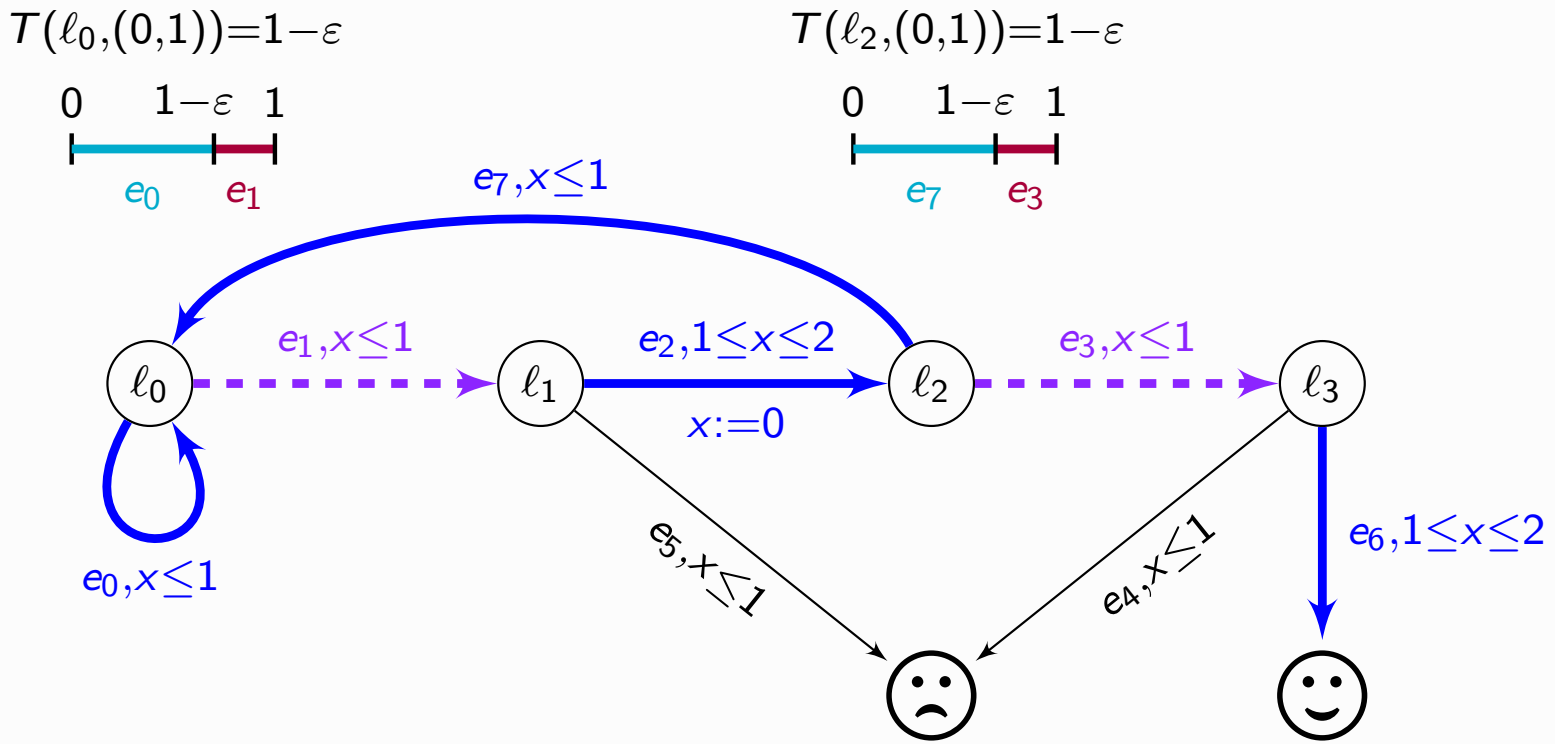
$T(\ell_0,(0,1))=1-\varepsilon$



$$\sigma_T(\ell_0,\nu)=\begin{cases} e_0 & \text{if } \nu<1-\varepsilon \\ e_1 & \text{if } \nu\geq 1-\varepsilon \end{cases} \quad \rightsquigarrow \quad \mathbb{P}^{s_0}_{\sigma_T}\left((\mathcal{A},\mu)\models \Diamond \text{☺}\right)\geq 1-\varepsilon.$$

About the construction of T

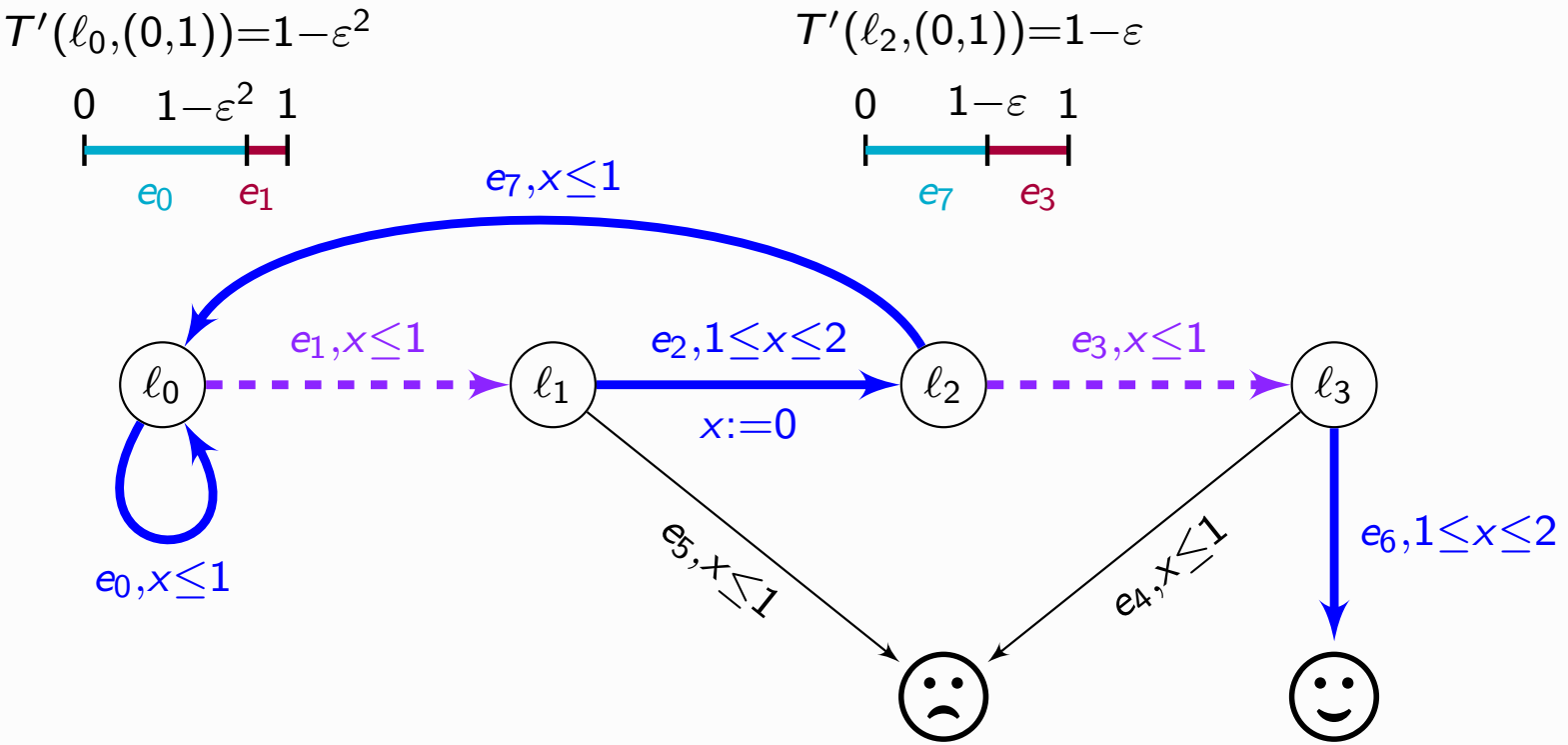
A not so simple case (uniform distributions)



$$\mathbb{P}_{\sigma_T}([\ell_0, 0] \models \Diamond F) < 2/3.$$

About the construction of T

A not so simple case (uniform distributions)



$$\mathbb{P}_{\sigma_T}([\ell_0, 0] \models \Diamond F) < 2/3.$$

However, ☺ is limit-surely reachable from $[\ell_0, 0]$, needs T'.

Conclusion and future work

- Conclusion
  - Algorithm in PTime for the almost-sure reachability problem on one-clock DSTA
  - Algorithm in PTime for the limit-sure reachability problem on one-clock DSTA
  - A symbolic representation of one-clock DSTA via finite MDP.
- Future work
  - Other winning conditions (Büchi,...)
  - Consider the 2-$\frac{1}{2}$ players framework.
  - ...