# Probabilistic Disclosure: Maximisation vs. Minimisation

Béatrice Bérard, Serge Haddad, Engel Lefaucheux

LSV, ENS Paris-Saclay& IRISA, Rennes & CNRS & Inria, France

Verification group, IRIF, January the 29th 2018

# Opacity

Opacity is achieved when an external observer cannot be sure that a *secret behaviour* has occurred.

Applicable to several information flow properties:

- anonymity
- non interference
- conditional declassification

# A Framework for Opacity

A system $\mathcal{S}$ produces behaviours: $\rho \in \mathcal{B}(\mathcal{S})$

Some of them are secret: $Sec \subseteq \mathcal{B}(\mathcal{S})$

A passive attacker observes the system: $\mathsf{O}(\rho)$

# A Framework for Opacity

A system $\mathcal{S}$ produces behaviours: $\rho \in \mathcal{B}(\mathcal{S})$

Some of them are secret: $Sec \subseteq \mathcal{B}(\mathcal{S})$

A passive attacker observes the system: $\mathsf{O}(\rho)$

**Qualitative problem.**

Does there exist a run that *discloses* the secret: $\mathsf{O}^{-1}(\mathsf{O}(\rho)) \subseteq Sec$?

# A Framework for Opacity

A system $\mathcal{S}$ produces behaviours: $\rho \in \mathcal{B}(\mathcal{S})$

Some of them are secret: $Sec \subseteq \mathcal{B}(\mathcal{S})$

A passive attacker observes the system: $\mathsf{O}(\rho)$

**Qualitative problem.**

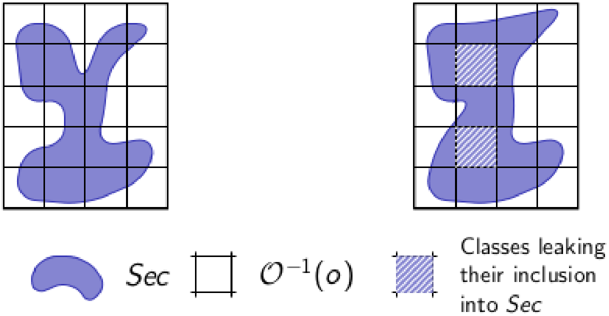
Does there exist a run that *discloses* the secret: $\mathsf{O}^{-1}(\mathsf{O}(\rho)) \subseteq Sec$?

**Quantitative problem.**

What is the "measure" of runs that disclose the secret?

Requires a distribution on the behaviours

# Illustration



With $\overline{Sec} = Path(\mathcal{A}) \setminus Sec$:
No disclosing path iff
$V = Sec \setminus \mathsf{O}^{-1}(\mathsf{O}(\overline{Sec}))$ is empty

Measuring the disclosure set $V$

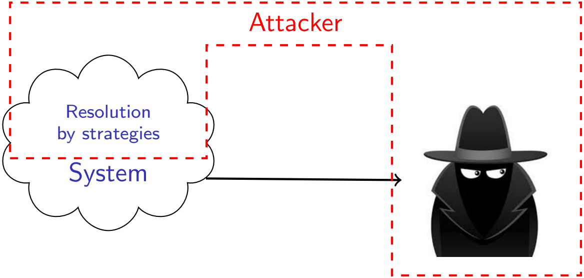
# Active Disclosure

**Active attacker.**

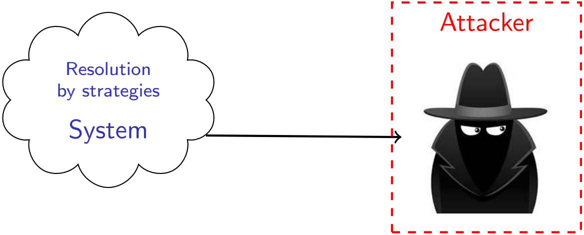
The attacker consists of two components

- The passive external observer;
- Some piece of code that is inside the system (worm, Trojan horse, etc.).

How to maximise disclosure?



# Active Disclosure



**System designer.**

The designer has provided a first version securing the required functionalities.

He must develop the access policy.

How to minimise disclosure?

# Active Disclosure

**Active attacker.**

The attacker consists of two components

- The passive external observer;
- Some piece of code that is inside the system (worm, Trojan horse, etc.).

How to maximise disclosure?

**System designer.**

The designer has provided a first version securing the required functionalities.

He must develop the access policy.

How to minimise disclosure?

# Outline

1. Semantics

2. Maximisation for Finite Horizon

3. Minimisation for Finite Horizon

4. Fixed Horizon

# Outline

1 Semantics

**Maximisation for Finite Horizon**

**Minimisation for Finite Horizon**

**Fixed Horizon**

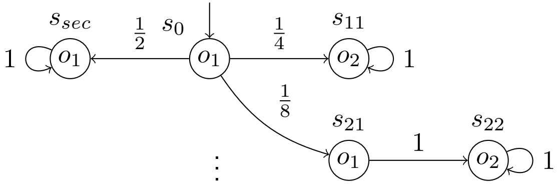
# Observable Markov Chain

**An observable Markov chain $\mathcal{M}$ consists of:**

- $S$, a countable set of states;
- $p : S \to \mathsf{Dist}(S)$, a transition function;
- $\mathsf{O} : S \to \Sigma \cup \{\varepsilon\}$ an observation function;
- an initial distribution $\mu_0$.

One only considers *convergent* Markov chains (no loop of unobservable states).

A run $\rho = s_0 s_1 \ldots$ is a sequence of states such that for all $i$, $p(s_{i+1}|s_i) > 0$.

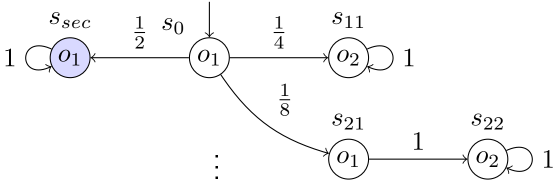


# Secret and Disclosure

Let $Sec \subseteq S$, be a set of absorbing *secret* states.

A run $\rho = s_0 s_1 \ldots$ is a *secret run* if for some $i$, $s_i \in Sec$.

A sequence of observations $w$ *discloses* the secret
if for all run $\rho \in \mathsf{O}^{-1}(w)$, $\rho$ is a secret run.



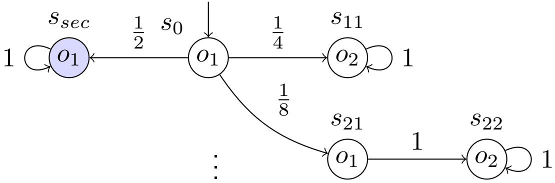
Let $Sec = \{s_{sec}\}$.

# Secret and Disclosure

Let $Sec \subseteq S$, be a set of absorbing *secret* states.

A run $\rho = s_0 s_1 \dots$ is a *secret run* if for some $i$, $s_i \in Sec$.

A sequence of observations $w$ *discloses* the secret
if for all run $\rho \in \mathsf{O}^{-1}(w)$, $\rho$ is a secret run.



Let $Sec = \{s_{sec}\}$. Then:

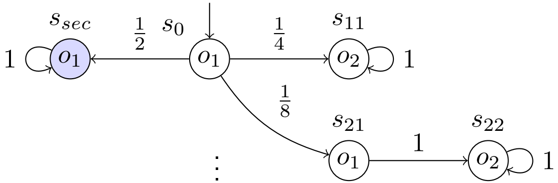
- $s_0 s_{sec}^{\omega}$ and for all $n$, $s_0 s_{sec}^{n}$ are secret runs.

# Secret and Disclosure

Let $Sec \subseteq S$, be a set of absorbing *secret* states.

A run $\rho = s_0 s_1 \dots$ is a *secret run* if for some $i$, $s_i \in Sec$.

A sequence of observations $w$ *discloses* the secret
if for all run $\rho \in \mathsf{O}^{-1}(w)$, $\rho$ is a secret run.

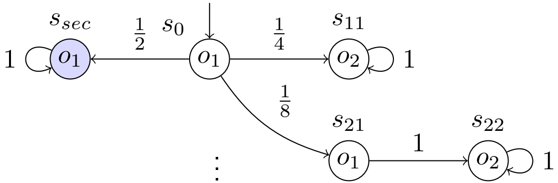


Let $Sec = \{s_{sec}\}$. Then:

- $s_0 s_{sec}^{\omega}$ and for all $n$, $s_0 s_{sec}^{n}$ are secret runs.
- $o_1^{\omega}$ discloses the secret and for all $n$, $o_1^{n}$ does not disclose the secret.

# Disclosure Probabilities

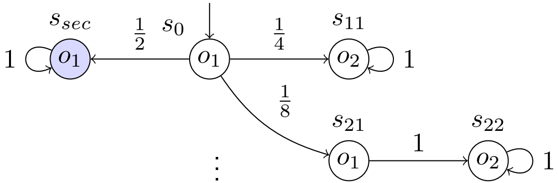
- The $\omega$-*disclosure*, $Disc_\omega(\mathcal{M}(\mu_0))$, is the probability of infinite disclosing observation sequences
- The *disclosure*, $Disc(\mathcal{M}(\mu_0))$, is the probability of *minimal disclosing* observation sequences.
- The $n$-*disclosure*, $Disc_n(\mathcal{M}(\mu_0))$, is the probability of disclosing observation sequences of length $n$.



$Disc_\omega(\mathcal{M}(\mu_0)) = \frac{1}{2}$ and $Disc_n(\mathcal{M}(\mu_0)) = Disc(\mathcal{M}(\mu_0)) = 0$.

# Disclosure Probabilities

- The $\omega$-*disclosure*, $Disc_\omega(\mathcal{M}(\mu_0))$, is the probability of infinite disclosing observation sequences
- The *disclosure*, $Disc(\mathcal{M}(\mu_0))$, is the probability of *minimal disclosing* observation sequences.
- The $n$-*disclosure*, $Disc_n(\mathcal{M}(\mu_0))$, is the probability of disclosing observation sequences of length $n$.



$Disc_\omega(\mathcal{M}(\mu_0)) = \frac{1}{2}$ and $Disc_n(\mathcal{M}(\mu_0)) = Disc(\mathcal{M}(\mu_0)) = 0$.

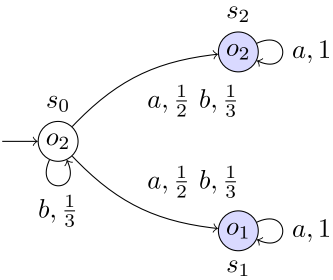
When $\mathcal{M}$ is finitely branching, $Disc_\omega(\mathcal{M}(\mu_0)) = Disc(\mathcal{M}(\mu_0))$

# Observable Markov Decision Process

**An observable Markov decision process (MDP)** M **consists of:**

- $S$, a finite set of states and secret states $Sec \subseteq S$;
- Act $= \cup_{s \in S} A(s)$ where $A(s)$ is a finite non empty set of actions;
- $p : S \times \mathsf{Act} \to \mathsf{Dist}(S)$, a transition function defined for $(s, a)$ when $a \in A(s)$;
- O : $S \to \Sigma \cup \{\varepsilon\}$ an observation function;
- an initial distribution $\mu_0$.

One considers convergent MDP.


$s_2$
$o_2$
$a, 1$
$s_0$
$a, \frac{1}{2}$ $b, \frac{1}{3}$
$o_2$
$a, \frac{1}{2}$ $b, \frac{1}{3}$
$b, \frac{1}{3}$
$o_1$
$a, 1$
$s_1$

# Strategies of Markov Decision Process

In order to obtain a randomised behaviour, one needs strategies.

A *strategy* $\sigma$ associates with all finite run $\rho$ ending in state $s = \mathsf{last}(\rho)$ a distribution over actions in $s$: $\sigma(\rho) \in \mathsf{Dist}(A(s))$.

# Strategies of Markov Decision Process

In order to obtain a randomised behaviour, one needs strategies.

A *strategy* $\sigma$ associates with all finite run $\rho$ ending in state $s = \mathsf{last}(\rho)$ a distribution over actions in $s$: $\sigma(\rho) \in \mathsf{Dist}(A(s))$.

- A strategy is *memoryless* if for all $\rho$, $\sigma(\rho)$ only depends on $\mathsf{last}(\rho)$;

# Strategies of Markov Decision Process

In order to obtain a randomised behaviour, one needs strategies.

A *strategy* $\sigma$ associates with all finite run $\rho$ ending in state $s = \text{last}(\rho)$ a distribution over actions in $s$: $\sigma(\rho) \in \text{Dist}(A(s))$.

- A strategy is *memoryless* if for all $\rho$, $\sigma(\rho)$ only depends on last$(\rho)$;
- A strategy is *deterministic* if for all $\rho$, $\sigma(\rho)$ is a Dirac distribution;

# Strategies of Markov Decision Process

In order to obtain a randomised behaviour, one needs strategies.

A *strategy* $\sigma$ associates with all finite run $\rho$ ending in state $s = \mathsf{last}(\rho)$ a distribution over actions in $s$: $\sigma(\rho) \in \mathsf{Dist}(A(s))$.

- A strategy is *memoryless* if for all $\rho$, $\sigma(\rho)$ only depends on $\mathsf{last}(\rho)$;
- A strategy is *deterministic* if for all $\rho$, $\sigma(\rho)$ is a Dirac distribution;
- A strategy is *observation-based* if for all $\rho$, $\sigma(\rho)$ only depends on $\mathsf{O}(\rho)$ and $\mathsf{last}(\rho)$.

# Strategies of Markov Decision Process

In order to obtain a randomised behaviour, one needs strategies.

A *strategy* $\sigma$ associates with all finite run $\rho$ ending in state $s = \mathsf{last}(\rho)$ a distribution over actions in $s$: $\sigma(\rho) \in \mathsf{Dist}(A(s))$.

- A strategy is *memoryless* if for all $\rho$, $\sigma(\rho)$ only depends on $\mathsf{last}(\rho)$;
- A strategy is *deterministic* if for all $\rho$, $\sigma(\rho)$ is a Dirac distribution;
- A strategy is *observation-based* if for all $\rho$, $\sigma(\rho)$ only depends on $\mathsf{O}(\rho)$ and $\mathsf{last}(\rho)$.

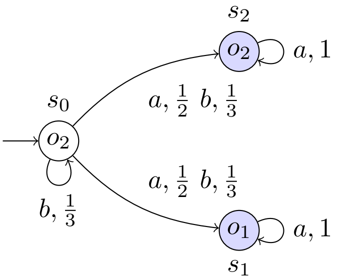
$B^{\sigma}_{\rho}$, the *belief* of $\rho$, is the set of possible states corresponding to the last observation of $\mathsf{O}(\rho)$.

A strategy is *belief-based* if for all $\rho$, $\sigma(\rho)$ only depends on $B^{\sigma}_{\rho}$ and $\mathsf{last}(\rho)$.

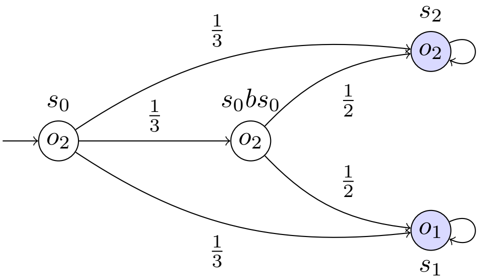
# From MDP to Markov Chains

Given an MDP $\mathsf{M}(\mu_0)$ and a strategy one obtains a Markov chain $\mathsf{M}_\sigma(\mu_0)$ whose states are $\sigma$-*compatible* runs of M.

Let $\sigma(s_0) = b$ and $\sigma(s_0 b s_0) = a$. Then:

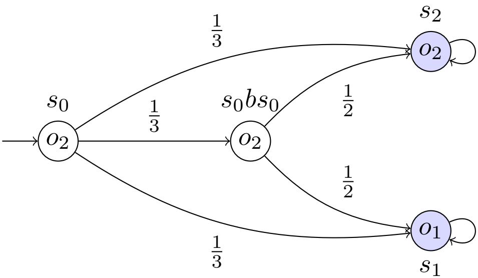


$s_2$
$o_2$
$a, 1$
$s_0$
$o_2$
$a, \frac{1}{2}$ $b, \frac{1}{3}$
$a, \frac{1}{2}$ $b, \frac{1}{3}$
$b, \frac{1}{3}$
$o_1$
$a, 1$
$s_1$



# Disclosure in MDP

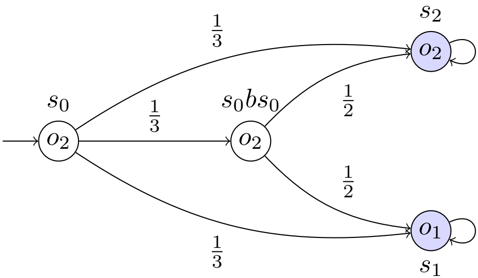
The disclosures of $\mathsf{M}(\mu_0)$ w.r.t. strategy $\sigma$ are the disclosures of $\mathsf{M}_\sigma(\mu_0)$.



Here $Disc_1 = 0$

# Disclosure in MDP

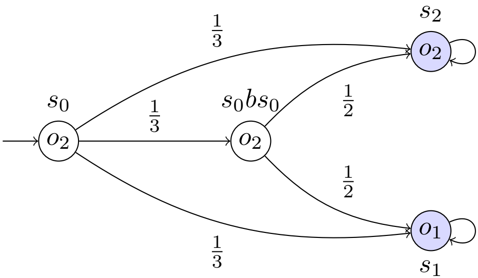
The disclosures of $\mathsf{M}(\mu_0)$ w.r.t. strategy $\sigma$ are the disclosures of $\mathsf{M}_\sigma(\mu_0)$.



Here $Disc_1 = 0$, $Disc_2 = \frac{1}{3}$

# Disclosure in MDP

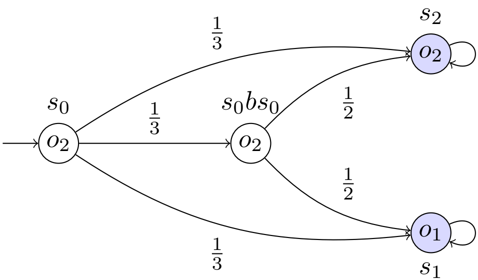
The disclosures of M$(\mu_0)$ w.r.t. strategy $\sigma$ are the disclosures of M$_\sigma(\mu_0)$.



Here $Disc_1 = 0$, $Disc_2 = \frac{1}{3}$ and $Disc_3 = Disc = 1$.

# Disclosure in MDP

The disclosures of $\mathsf{M}(\mu_0)$ w.r.t. strategy $\sigma$ are the disclosures of $\mathsf{M}_\sigma(\mu_0)$.

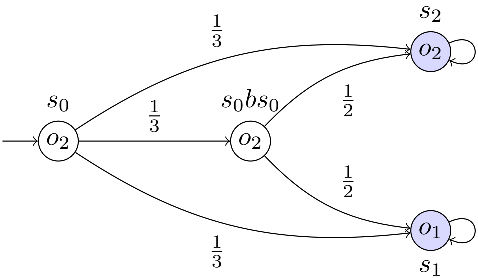


Here $Disc_1 = 0$, $Disc_2 = \frac{1}{3}$ and $Disc_3 = Disc = 1$.

Depending whether the agent is the system or the attacker,
one looks for supremum or infimum over strategies.

# Disclosure in MDP

The disclosures of $\mathsf{M}(\mu_0)$ w.r.t. strategy $\sigma$ are the disclosures of $\mathsf{M}_\sigma(\mu_0)$.



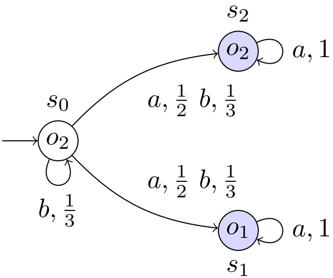
Here $Disc_1 = 0$, $Disc_2 = \frac{1}{3}$ and $Disc_3 = Disc = 1$.

Depending whether the agent is the system or the attacker,
one looks for supremum or infimum over strategies.

For all strategy there is an observation-based strategy with same disclosure.

# Previous Works

- [Bérard, Chatterjee, Sznajder IPL 2015] considers the attacker point of view assuming *the observer is not aware of the strategy*.

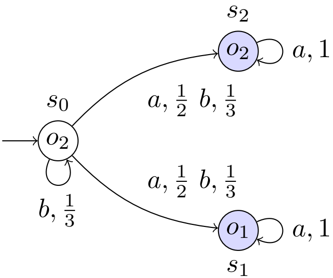


$s_2$
$o_2$
$a, 1$
$s_0$
$o_2$
$a, \frac{1}{2}$ $b, \frac{1}{3}$
$a, \frac{1}{2}$ $b, \frac{1}{3}$
$b, \frac{1}{3}$
$o_1$
$a, 1$
$s_1$

With our definition, maximal disclosure is 1 while with the previous one it is $\frac{1}{2}$.

# Previous Works

- [Bérard, Chatterjee, Sznajder IPL 2015] considers the attacker point of view assuming *the observer is not aware of the strategy*.

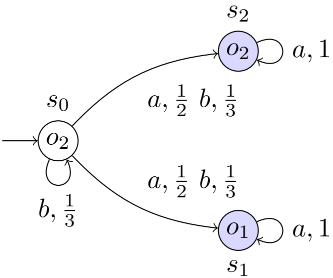

$s_2$
$o_2$
$a, 1$
$a, \frac{1}{2}$ $b, \frac{1}{3}$
$s_0$
$o_2$
$b, \frac{1}{3}$
$a, \frac{1}{2}$ $b, \frac{1}{3}$
$o_1$
$a, 1$
$s_1$

With our definition, maximal disclosure is 1 while with the previous one it is $\frac{1}{2}$.

Security should not be based on the black box hypothesis!

# Previous Works

- [Bérard, Chatterjee, Sznajder IPL 2015] considers the attacker point of view assuming *the observer is not aware of the strategy*.


$s_2$
$o_2$
$a, 1$
$a, \frac{1}{2}$ $b, \frac{1}{3}$
$s_0$
$o_2$
$a, \frac{1}{2}$ $b, \frac{1}{3}$
$b, \frac{1}{3}$
$o_1$
$a, 1$
$s_1$

With our definition, maximal disclosure is 1 while with the previous one it is $\frac{1}{2}$.

Security should not be based on the black box hypothesis!

- [Bérard, Kouchnarenko, Mullins, Sassolas WODES 2016] proposes a restricted framework based on interval Markov chains where both definitions coincide.

# Disclosure Problems

**Computation problems.**

- The *value problem*: compute the disclosure;
- The *strategy problem*: compute an optimal strategy whenever it exists.

**Quantitative decision problems.**

- The *disclosure problem*: Given M and a threshold $\theta \in [0, 1]$, is $disc(\mathsf{M}) \bowtie \theta$? with $\bowtie = \geq$ (resp. $\bowtie = \leq$) for maximisation (resp. for minimisation)
- the *strategy decision problem*: does there exist a strategy $\sigma$ such that $disc(\mathsf{M}_\sigma) \bowtie \theta$?

**Qualitative decision problems.**

- The *limit-sure disclosure problem*: the disclosure problem when $\theta = 1$ for maximisation and $\theta = 0$ for minimisation
- The *almost-sure disclosure problem*: the strategy decision problem with the same restrictions.

# Outline

Semantics

2 Maximisation for Finite Horizon

Minimisation for Finite Horizon

Fixed Horizon

# Deterministic Strategies are Enough

**Sketch of Proof.**

Pick $\sigma$ an arbitrary strategy.

Let $\varphi^\sigma$ be the property of $\sigma$-compatible runs defined by:

$$\rho \models \varphi^\sigma \text{ if } \rho \text{ discloses the secret.}$$

**Observation.** $\varphi^\sigma$ only depends on the set of $\sigma$-compatible runs and is regular.

Applying [Chatterjee et al, MFCS 2010], there is a deterministic strategy $\sigma'$ such that:

- $\mathbf{P}^{\sigma'}(\rho \models \varphi^\sigma) \geq \mathbf{P}^{\sigma}(\rho \models \varphi^\sigma)$
- The set of $\sigma'$-compatible runs is included in the set of $\sigma$-compatible runs.

So for $\rho$, $\sigma'$-compatible, $\rho \models \varphi^\sigma$ implies $\rho \models \varphi^{\sigma'}$.

Thus:

$$\mathbf{P}^{\sigma'}(\rho \models \varphi^{\sigma'}) \geq \mathbf{P}^{\sigma'}(\rho \models \varphi^\sigma) \geq \mathbf{P}^{\sigma}(\rho \models \varphi^\sigma)$$

# Deterministic Strategies are Enough

**Sketch of Proof.**

Pick $\sigma$ an arbitrary strategy.

Let $\varphi^\sigma$ be the property of $\sigma$-compatible runs defined by:

$$\rho \models \varphi^\sigma \text{ if } \rho \text{ discloses the secret.}$$

**Observation.** $\varphi^\sigma$ only depends on the set of $\sigma$-compatible runs and is regular.

Applying [Chatterjee et al, MFCS 2010],
there is a deterministic strategy $\sigma'$ such that:

- $\mathbf{P}^{\sigma'}(\rho \models \varphi^\sigma) \geq \mathbf{P}^\sigma(\rho \models \varphi^\sigma)$
- The set of $\sigma'$-compatible runs is included in the set of $\sigma$-compatible runs.

So for $\rho$, $\sigma'$-compatible, $\rho \models \varphi^\sigma$ implies $\rho \models \varphi^{\sigma'}$.

Thus:

$$\mathbf{P}^{\sigma'}(\rho \models \varphi^{\sigma'}) \geq \mathbf{P}^{\sigma'}(\rho \models \varphi^\sigma) \geq \mathbf{P}^\sigma(\rho \models \varphi^\sigma)$$

This proof does not work for minimisation.

# Results

**Disclosure problem and limit-sure disclosure problem for maximisation are undecidable.**

- Reduction from emptiness and value 1 problem from probabilistic automata.

# Results

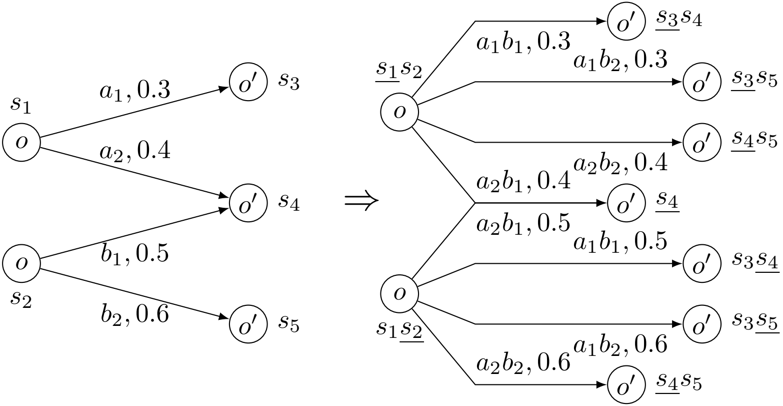
**Disclosure problem and limit-sure disclosure problem for maximisation are undecidable.**

- Reduction from emptiness and value 1 problem from probabilistic automata.

**The almost-sure disclosure problem for maximisation is EXPTIME-complete.**

- Hardness through reduction from the safety problem in games with imperfect information,
- Algorithm based on POMDP techniques.

# Illustration for Almost Sure Disclosure



POMDP restriction on strategies ensures

that the same tuple of actions is chosen in states of the belief.

Result on deterministic strategies ensures that beliefs are correct.

Thus disclosure reduces to reachability of $\{(s, B)\}$ with $B \subseteq Sec$.

# Outline

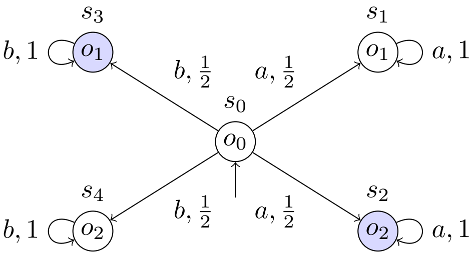
Semantics

Maximisation for Finite Horizon

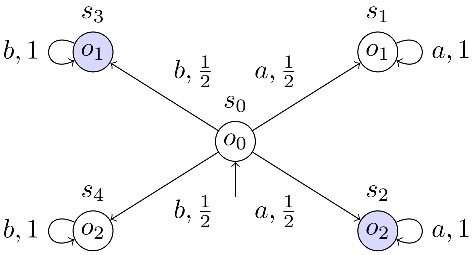
3 Minimisation for Finite Horizon

Fixed Horizon

# Deterministic Strategies are not Enough

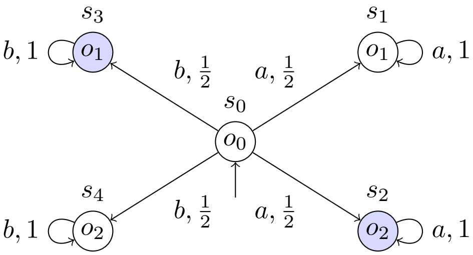


# Deterministic Strategies are not Enough



Selecting $a$ or $b$ leads to a disclosure of $\frac{1}{2}$.

# Deterministic Strategies are not Enough



Selecting $a$ or $b$ leads to a disclosure of $\frac{1}{2}$.

Selecting $pa + (1-p)b$ for any $0 < p < 1$ leads to a disclosure of $0$.

# Almost Deterministic Strategies

How to address the previous issue?

# Almost Deterministic Strategies

How to address the previous issue?

**Almost deterministic decision rules.**

Let $\delta$ be the deterministic decision rule for state $s$ selecting action $a$.

Then $\delta_\varepsilon$ is a $\varepsilon$-decision rule defined by:

1. If $|A_s| > 1$ then $\delta_\varepsilon(a) = 1 - \varepsilon$ and for all $b \in A_s \setminus \{a\}$, $\delta(b) = \frac{\varepsilon}{|A_s|-1}$;
2. Else $\delta_\varepsilon(a) = 1$.

We say that $\delta_\varepsilon$ *favours* $\delta(s)$.

# Almost Deterministic Strategies

How to address the previous issue?

**Almost deterministic decision rules.**

Let $\delta$ be the deterministic decision rule for state $s$ selecting action $a$.

Then $\delta_\varepsilon$ is a $\varepsilon$-decision rule defined by:

1. If $|A_s| > 1$ then $\delta_\varepsilon(a) = 1 - \varepsilon$ and for all $b \in A_s \setminus \{a\}$, $\delta(b) = \frac{\varepsilon}{|A_s|-1}$;
2. Else $\delta_\varepsilon(a) = 1$.

We say that $\delta_\varepsilon$ *favours* $\delta(s)$.

**Almost deterministic strategies.**

Let $\sigma$ be an observation-based deterministic strategy.

Then $\{\sigma_\varepsilon\}_{\varepsilon>0}$ is a family of almost deterministic strategies defined by:

$$\sigma_\varepsilon(o_1 \dots o_n, s) = \sigma(o_1 \dots o_n, s)_{2^{-n}\varepsilon}$$

# Value Problem Analysis

**First step.**

Showing that families of almost deterministic strategies are dominant.

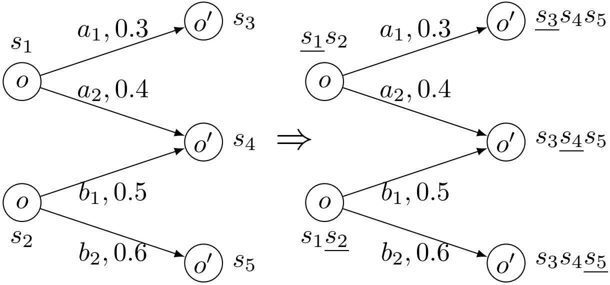
# Value Problem Analysis

**First step.**

Showing that families of almost deterministic strategies are dominant.

**Second step.**

Building an MDP mimicking the behaviour of almost deterministic strategies.



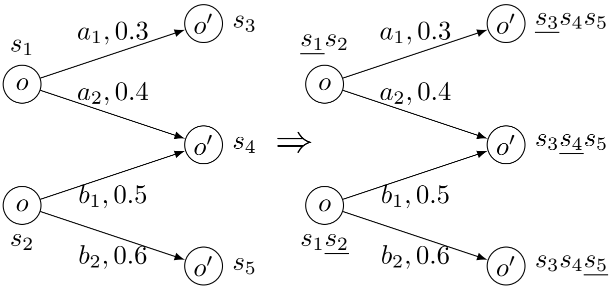
# Value Problem Analysis

**First step.**

Showing that families of almost deterministic strategies are dominant.

**Second step.**

Building an MDP mimicking the behaviour of almost deterministic strategies.



**Third step.** Minimal reachability is computable in polynomial time in the size of the MDP.

# Outline

Semantics

Maximisation for Finite Horizon

Minimisation for Finite Horizon

4 Fixed Horizon

# Fixed Horizon

**Value problem for maximisation is PSPACE-complete.**

- More efficient than using the POMDP translation,
- Hardness with reduction from Q3SAT,
- Determinism implies existence of a strategy.

# Fixed Horizon

**Value problem for maximisation is PSPACE-complete.**

- More efficient than using the POMDP translation,
- Hardness with reduction from Q3SAT,
- Determinism implies existence of a strategy.

**Value and strategy decision problems for minimisation.**

- The value problem is very similar to the maximal case *(except for the belief update)*
- The strategy problem requires to show that it is enough to restrict guesses over *equidistributed* decision rules.

Both are PSPACE-complete.

# Conclusion and Perspectives

## Contributions

- Revisiting the semantics of probabilistic disclosure
- Solving open issues for the maximisation problems
- Addressing the minimisation problems and establishing contrasted results

# Conclusion and Perspectives

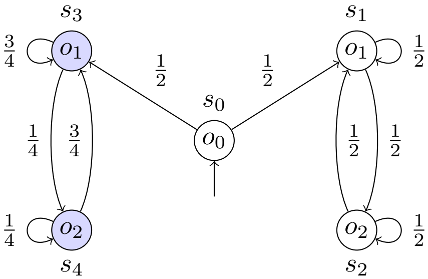
## Contributions

- Revisiting the semantics of probabilistic disclosure
- Solving open issues for the maximisation problems
- Addressing the minimisation problems and establishing contrasted results

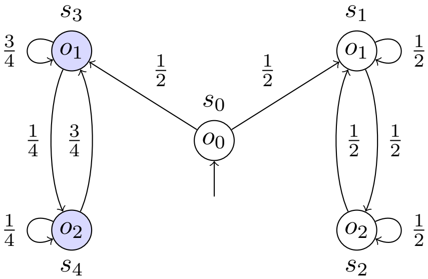
## Perspectives

- Closing the complexity gap for the minimisation within finite horizon
- Generalising the analysis of disclosure to hyperproperties
- Looking for decidable notions of approximate opacity

# Approximate Opacity

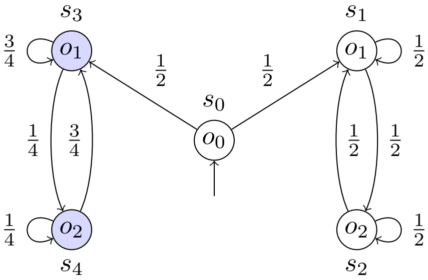


# Approximate Opacity



More '$a$' than '$b$' implies high probability of being secret.

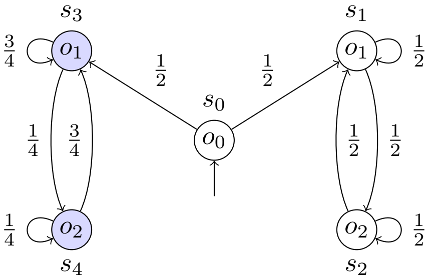
# Approximate Opacity



More '$a$' than '$b$' implies high probability of being secret.

Secret disclosed if doubt below a threshold $\lambda > 0$.

# Approximate Opacity



More '$a$' than '$b$' implies high probability of being secret.

Secret disclosed if doubt below a threshold $\lambda > 0$.

Secret disclosed for an infinite run if the doubt converges to $0$.

# Some other models

**Probabilistic automaton (PA).**

- A probabilistic automaton is a MDP with final states with a blind agent.
- So strategies are words.

The following problems are undecidable.

- Given a threshold $\theta$, does there exist a word such that its acceptance probability is at least $\theta$?
- Does there exist a family of words $\{w_n\}_{n\in\mathbb{N}}$ such that the sequence of their acceptance probabilities converges to 1?

# Some other models

**Probabilistic automaton (PA).**

- A probabilistic automaton is a MDP with final states with a blind agent.
- So strategies are words.

The following problems are undecidable.

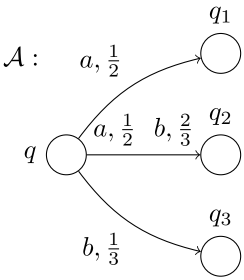
- Given a threshold $\theta$, does there exist a word such that its acceptance probability is at least $\theta$?
- Does there exist a family of words $\{w_n\}_{n\in\mathbb{N}}$ such that the sequence of their acceptance probabilities converges to 1?

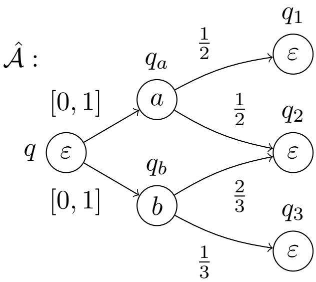
**Interval Markov Chain (IMC).**

- In an IMC, the probability transitions are specified by intervals.
- An IMC is a compact MDP where the actions allowed in a state are the vertices of the polytope defined by the intervals outgoing the state.

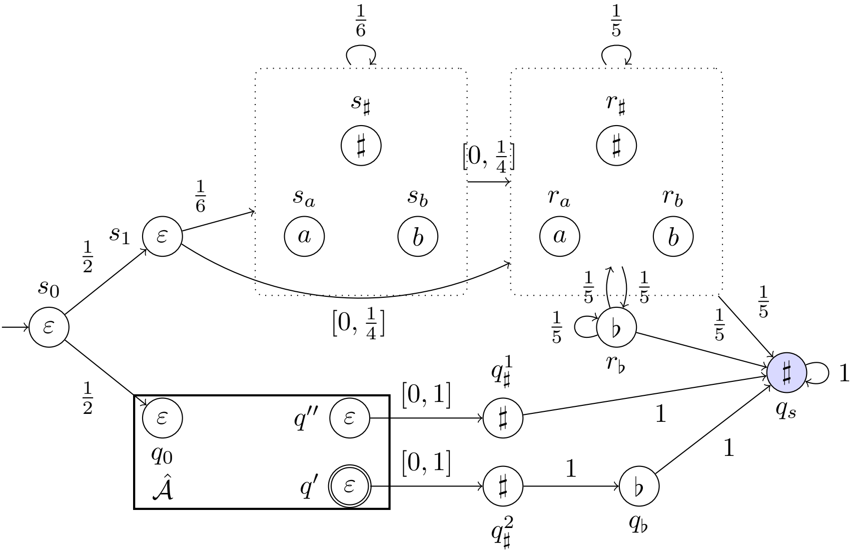
# A first reduction from PA to IMC

The alphabet of the PA becomes the alphabet of observations.





# A second reduction from PA to IMC



There exists a word with acceptance probability greater that $\frac{1}{2}$ iff the disclosure is greater than $\frac{1}{4}$.

# From the word to the strategy

Assume there exists a word $w = a_1 \dots a_n \in \{a, b\}^*$
accepted with probability greater than $\frac{1}{2}$ in $\mathcal{A}$.

Strategy $\sigma$ is defined as follows.

- In the lower part, $\sigma$ produces $w$ in $\hat{\mathcal{A}}$ and exits $\hat{\mathcal{A}}$ producing the observation sequence $w\sharp\flat\sharp^+$ with probability greater that $\frac{1}{4}$.

- In the upper part,
  - as long as the sequence of observations is some strict prefix $a_1 \dots a_i$, $\sigma$ forbids to enter $r_{a_{i+1}}$.
  - If the sequence of observations is $w$, $\sigma$ forbids to enter $r_\sharp$.

So no run in the upper part may produce $w\sharp\flat\sharp^+$.

# From the strategy to the word

**Observations.**

- The runs of the upper part are never disclosing;
- The runs of the lower part are disclosing iff their observation sequence belong $w\sharp\flat\sharp^+$ and cannot be mimicked in the upper part.

Consider a strategy $\sigma$ with with disclosure greater than $\frac{1}{4}$.

Inductively build a run $\rho$ with observation sequence $w \in \Sigma^*$.

Initially $\rho = s_0 s_1$.

As long as $\sigma$ applied on run $\rho$ forbids to enter some $r_y$ with $y \in \{a, b\}$ *(there is at most one)*, $\rho$ is extended by $s_y$.

There are three cases:

- If the construction never stops there is no disclosure;
- If the construction stops since $\sigma$ does not forbid any $r_y$ there is no disclosure;
- If the construction stops since $\sigma$ forbids $r_\sharp$ then $w\sharp\flat\sharp^+$ is the single disclosure pattern which implies that $w$ is accepted with probability greater than $\frac{1}{2}$.