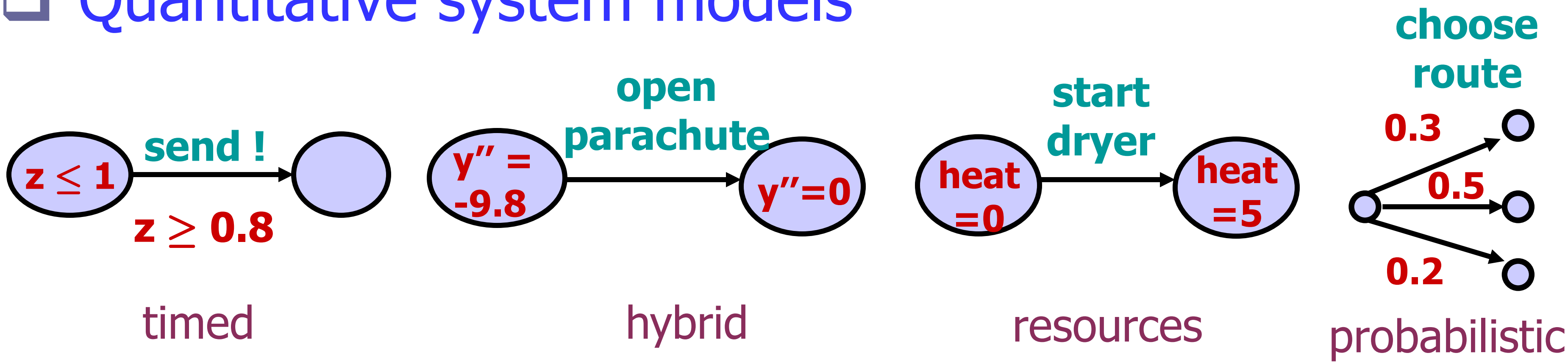
From Quality to Quantity: Logics and Metrics for Quantitative System models

Marielle Stoelinga
University of Twente

From Quality to Quantity

- Quantitative system models



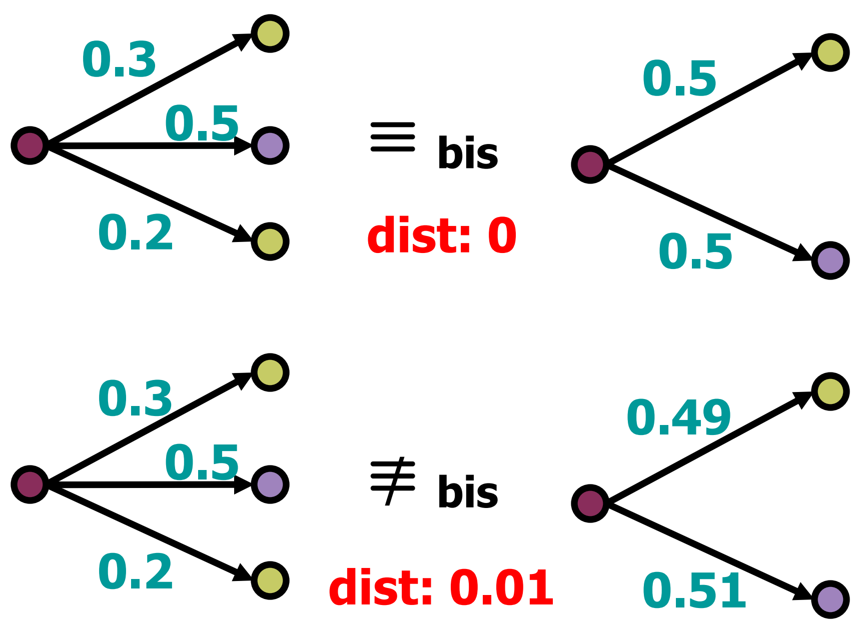
- Verification is usually boolean:
  - either **A** $\models \Phi$ or **A** $\not\models \Phi$
  - either **A** $\equiv_{\mathbf{bis}}$ **B** or **A** $\not\equiv_{\mathbf{bis}}$ **B**
- Problem:
  - lack of expressiveness: quantify our satisfaction
  - small perturbations have large effects

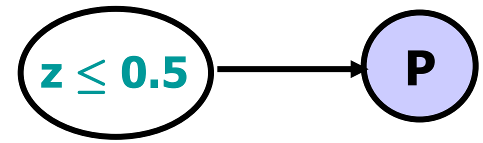
A $\models \Phi$ change values by 0.01 **A′** $\not\models \Phi$

A $\equiv_{\mathbf{bis}}$ **B** $\longrightarrow$ **A′** $\not\equiv_{\mathbf{bis}}$ **B**

fragility

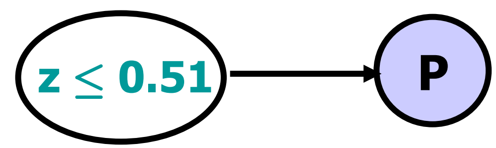
From Quality to Quantity





$\models \Diamond^{\leq 0.5} P$

$[\![A]\!](\Diamond^{\max} P) = 0.5$



$\models \Diamond^{\leq 0.5} P$

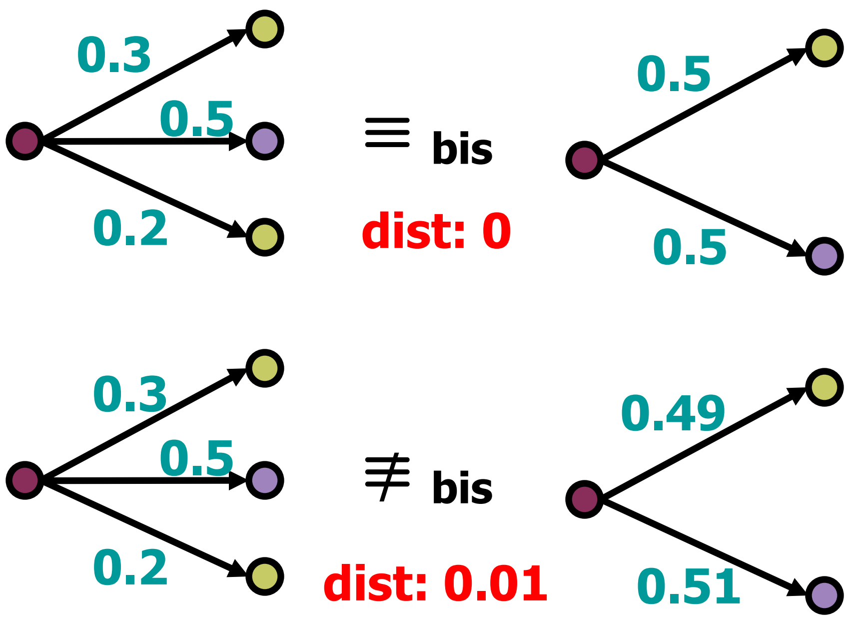
$[\![A]\!](\Diamond^{\max} P) = 0.51$

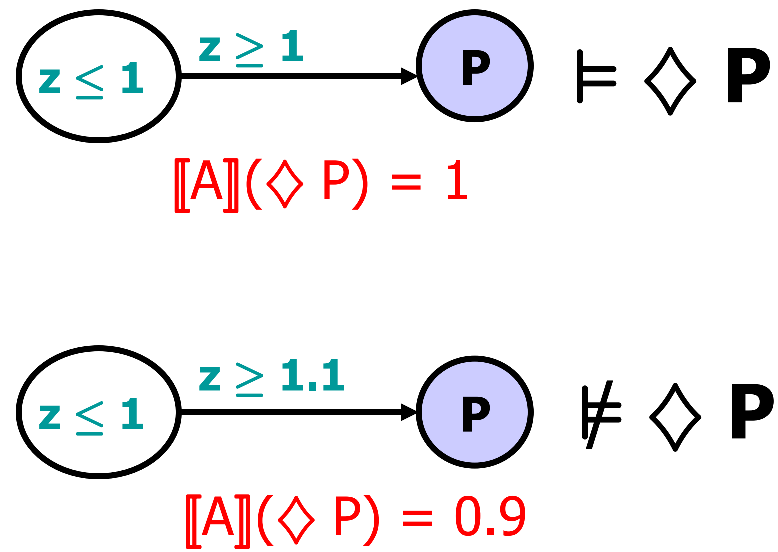
Our opinion: verification should be **quantitative**

- $A \models \phi \quad \rightsquigarrow \quad [\![A]\!](\phi) \in [0,1]$ how true is ϕ on **A**?
- $A \equiv_{bis} B \quad \rightsquigarrow$ dist(A,B) how similar are A and B?

  distance/metric

From Quality to Quantity





Quantitative system relations

- $s \sqsubseteq t \rightsquigarrow \mathrm{dist}(s,t)$

how similar are two systems?

- linear dist: trace inclusion/equiv
- branching dist: (bi-)simulation

Quantitative logics

- $s \models \phi \rightsquigarrow [\![\phi]\!](s) \in [0,1]$

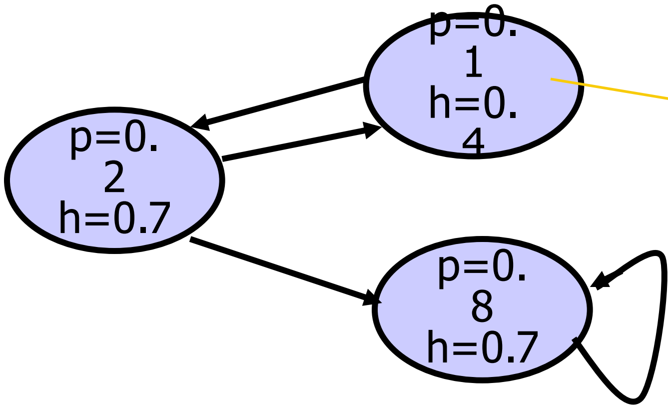
how true is ϕ in s?

- Quantitative LTL
- Quantitative CTL

The model

- First: QTSs
- Then: Stoc Games
- Others: real-time

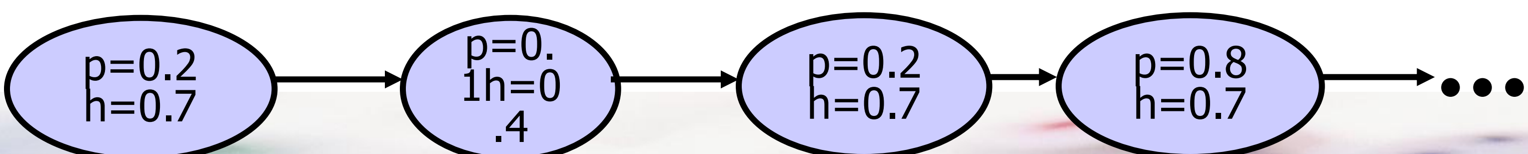
- Quantitative Transition Systems (QTSs)
  kripke structures with quantitative predicates



quantitative state predicates: each proposition has value in [0,1]

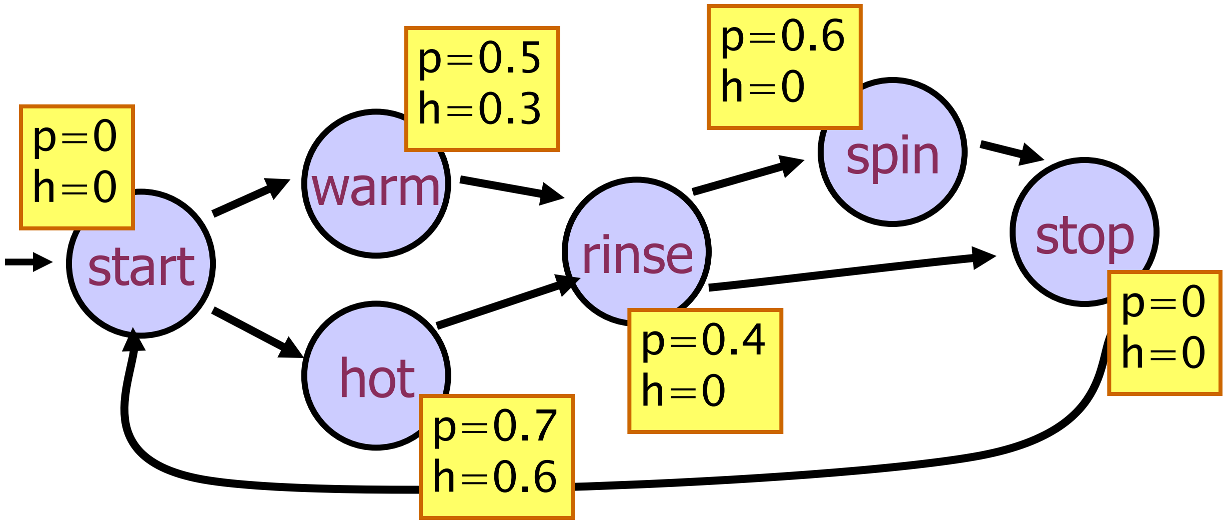
express: priorities, fuzzy predicates, rewards, power, heat, ...

- Semantics: quantitative traces



works as expected

Example: Kripke's Washing Machine



p = power
h = heating

Outline of this talk

- QTSs
  1. linear setting
     - linear distance ld
     - QLTL
  2. branching setting
     - branching distance bd
     - QCTL
- Stochastic Games
  3. branching setting
     - a priori distance
     - a posteriori distance
     - Qμ-calculus
- Conclusions

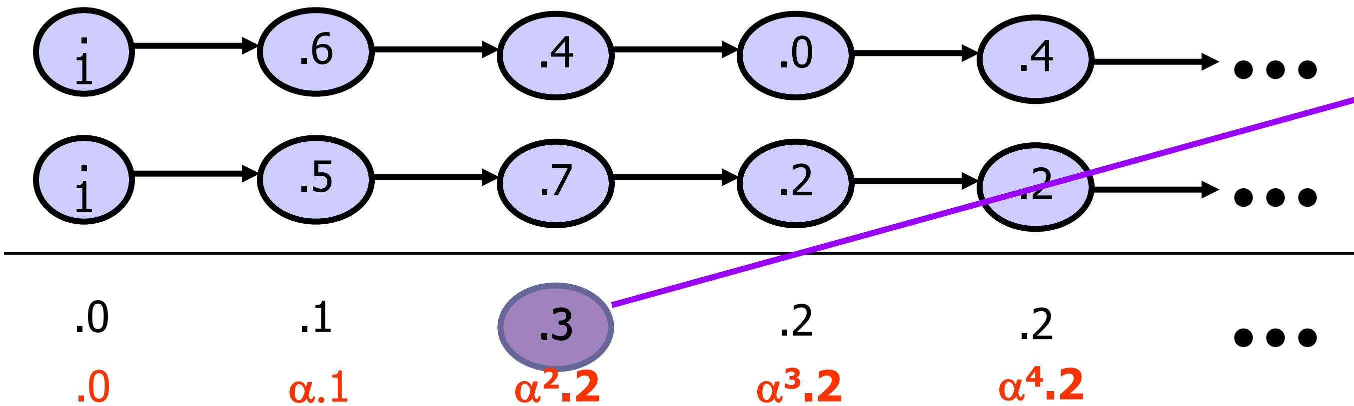
Linear Distances (trace inclusion/equivalence)

- How different are two states? *Propositional distance*

pd(p=0.1 q=0.8 , p=0.3 q=0.7) = 0.2

$$pd(s,t) = \max_{p \in \Sigma} |s(p) - t(p)|$$

- How different are two traces? *Trace distance*



$$ld^{<}(\sigma,\rho) = \sup_i pd^a(\sigma_i,\rho_i)$$

discounting

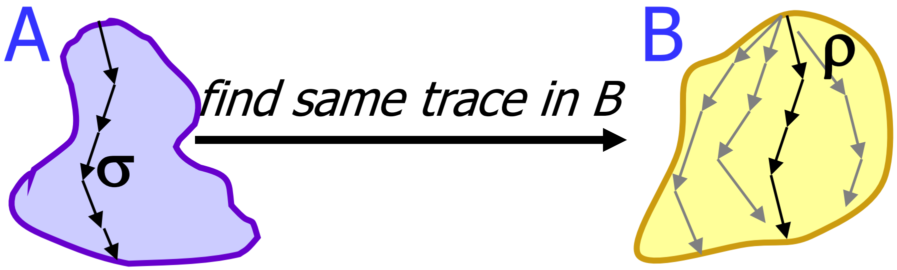
- How different are two systems? *Hausdorff set distance*

$$ld^{=}(A,B) = \sup_{\sigma \in \mathbf{tr(A)}} \inf_{\rho \in \mathbf{tr(B)}} ld^{s}(\sigma,\rho)$$

.... see next slide ....

Linear Distances

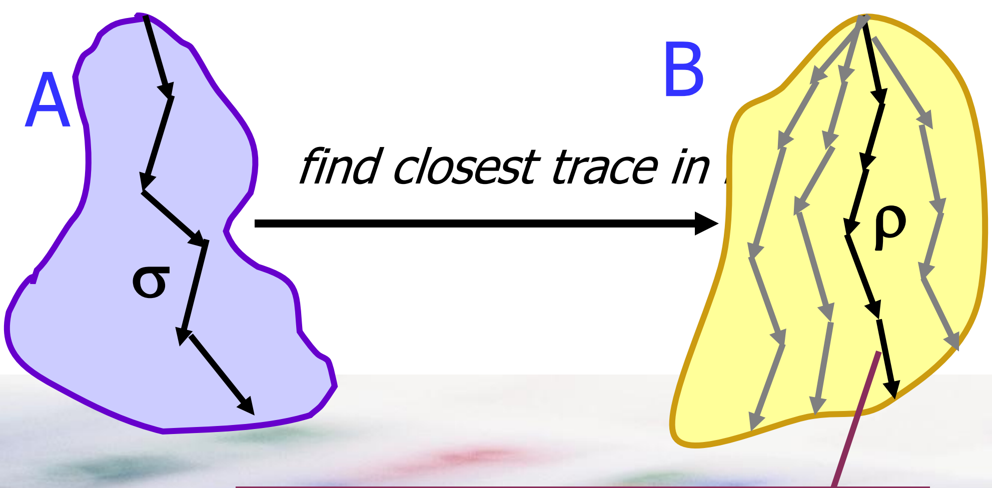
Trace inclusion: $A \sqsubseteq_{tr} B \;=\; tr(A) \subseteq tr(B)$



$A \sqsubseteq_{tr} B \;=$
$\quad \forall\, \sigma \in \mathbf{tr(A)}\ \exists \rho \in \mathbf{tr(B)}.\ \sigma = \rho$

$A =_{tr} B \;=$
$\quad A \sqsubseteq_{tr} B \ \&\ B \sqsubseteq_{tr} A$

Linear distance: $ld^{<}(A,B)$



$=$ trace at min dist

$= \;\mathbf{inf}_{\rho \in tr(B)}\, ld^{<}(\sigma,\rho)$

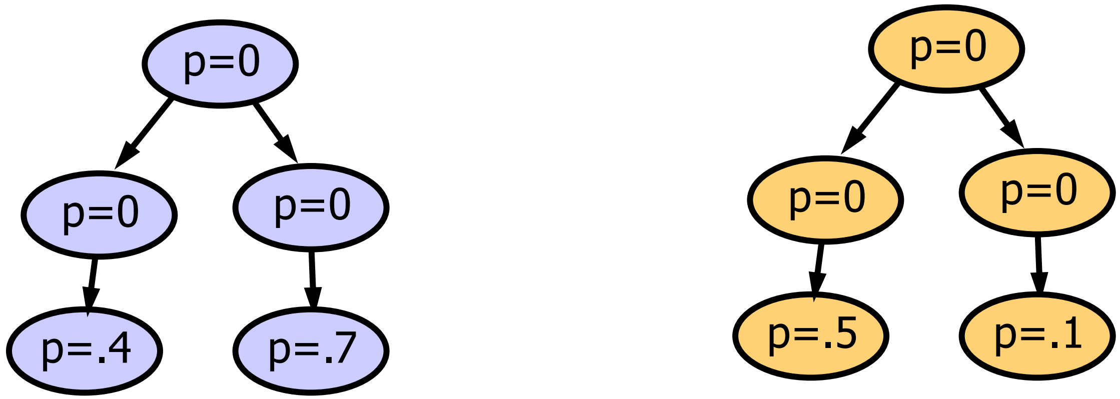
Find hardest trace in A to match

$ld^{<}(A,B) =$
$\quad \sup_{\sigma \in tr(A)} \inf_{\rho \in tr(B)} ld^{s}(\sigma,\rho)$

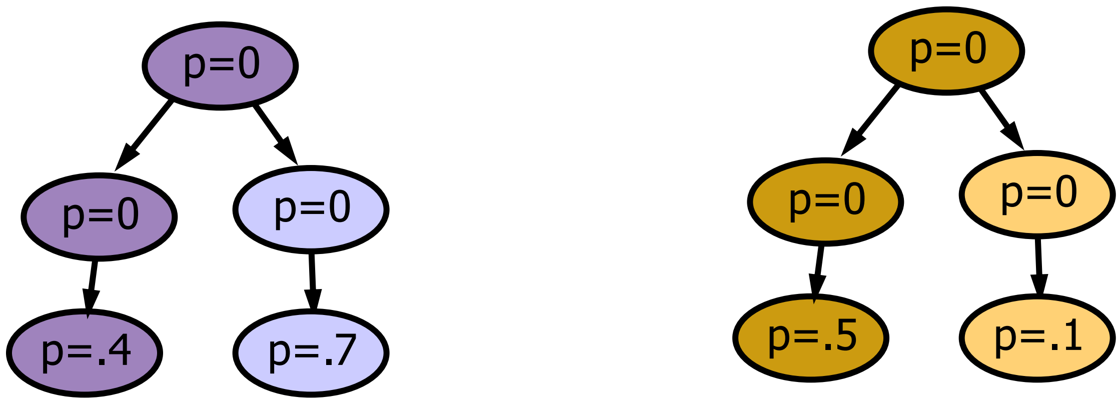
symmetric variant

$ld^{=}(A,B) =$
$\quad \max(\, ld^{<}(A,B),\, ld^{<}(B,A))$

$Ld^{<}(A,B)$: example



dist: .2



dist: .1

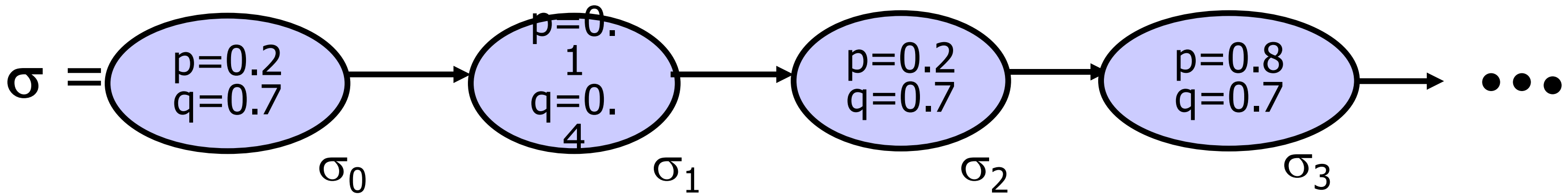
dist: .2

Quantitative Linear Time Logic (QLTL)

- (minimal) syntax

$$\Phi := \; p \mid \Phi \vee \Phi \mid \neg\, \Phi \mid \bigcirc\, \Phi \mid \Diamond\, \Phi \mid \Phi \oplus c \qquad c \in [0,1]$$

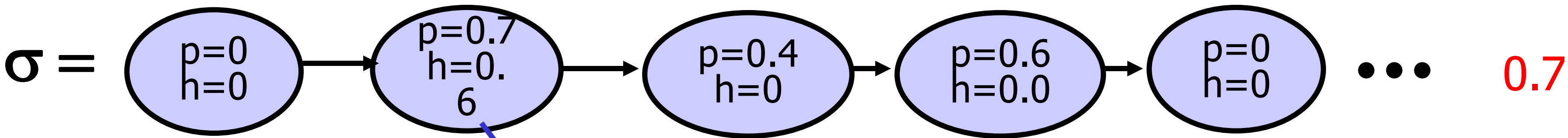
- semantics



- $[\![p]\!](\sigma) \;=\; \sigma_0(p)$
- $[\![\neg\, \Phi]\!](\sigma) \;=\; 1 - [\![\Phi]\!](\sigma)$
- $[\![\bigcirc\, \Phi]\!](\sigma) \;=\; [\![\Phi]\!](\sigma^1)$
- $[\![\Phi_1 \vee \Phi_2]\!](\sigma) \;=\; \max(\, [\![\Phi_1]\!](\sigma) \,,\, [\![\Phi_2]\!](\sigma) \,)$
- $[\![\Diamond\, \Phi]\!](\sigma) \;=\; \sup_i [\![\Phi]\!](\sigma^i)$
- $[\![\Phi \oplus c]\!](\sigma) \;=\; \min(\, [\![\Phi]\!](\sigma) + c, 1)$

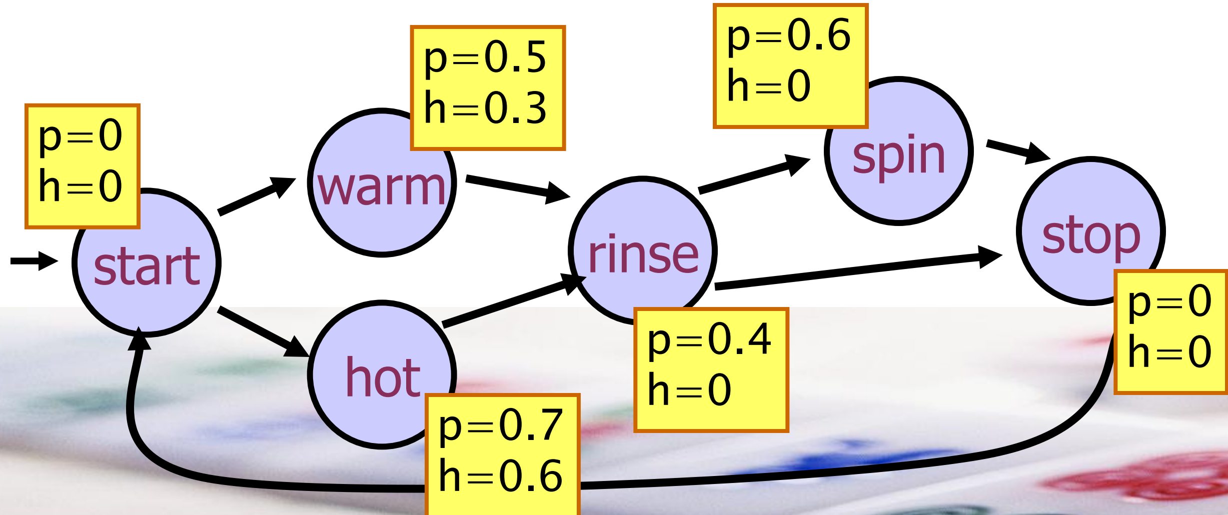
$$[\![\Phi]\!](s) = \inf_{\sigma \in tr(s)} [\![\Phi]\!](\sigma)$$

Semantics for ◇ p



$[\![\lozenge\, p]\!](\sigma) = \sup_i\, (\sigma^i)\,(p) = 0.7$

Washing Machine



$[\![\lozenge\, p]\!](s) =$
$\inf_\sigma [\![\lozenge\, p]\!]\, (\sigma) =$
0.6

$\lozenge\, p = 0.6$

min peak consumption

Linear Characterization Results

- **boolean:**

  $A \equiv_{tr} B$ iff $\forall \phi \in LTL.\ A \models \phi \Leftrightarrow B \models \phi$

  $A \sqsubseteq_{tr} B$ iff $\forall \phi \in LTL^{+}.\ A \models \phi \Rightarrow B \models \phi$

- **quantitative:**

  $ld^{=}(A, B) = \sup_{\Phi \in QLTL}.\ |\ [\![A]\!](\phi) - [\![B]\!](\phi)\ |$

  $ld^{<}(A, B) = \sup_{\Phi \in QLTL^{+}}.\ [\![A]\!](\phi) - [\![B]\!](\phi)$

$\oplus$ needed in Q-logics

Two directions:

- QLTL formulae cannot distinguish more than ld ($\geq$-direction)
- QLTL can distinguish arbitrary close to ld ($\leq$-direction)
  (only $\bigcirc$, $\oplus$ needed)

Part 2: Simulation Distance

Boolean simulation: $s \sqsubseteq_{sim} t$

R is a sim rel iff for all $(s,t) \in R$

1. $prop(s) \;=\; prop(t)$
2. $s \to s' \Rightarrow$
   $\exists t' \,.\, t \to t' \;\&\; (s',t') \in R$

$\to$ preserves R

$\sqsubseteq_{sim}$ is the largest sim rel

Simulation distance: $bd^{<}(s,t)$

d is a sim distance iff for all $d(s,t) = x$

1. $d(s,t) \;\geq\; pd(s,t)$
2. $s \to s' \Rightarrow$
   $\exists t' \,.\, t \to t' \;\&\; d(s',t') \leq x$

$\to$ preserves d

$bd^{<}$ is the smallest sim distance

$$s \sqsubseteq_{sim} t \;\text{ iff }\; bd^{<}(s,t) = 0$$

Simulation Distance

$bd^{<}$ is the smallest distance such that for $d(s,t) = x$

1. $d(s,t) \geq pd(s,t)$
2. $s \to s' \Rightarrow \exists\, t' \,.\, t \to t' \;\&\; d(s',t') \leq x$

1. $d(s,t) \geq pd(s,t)$
2. $s \to s' \Rightarrow \mathbf{min}_{t'\,.\,t \to t'}\; d(s',t') \leq x$

1. $d(s,t) \geq pd(s,t)$
2. $\mathbf{max}_{s'\,.\,s \to s'}\; \mathbf{min}_{t'\,.\,t \to t'}\; d(s',t') \leq x$

1. $pd(s,t) \leq d(s,t)$
2. $\mathbf{max}_{s'\,.\,s \to s'}\; \mathbf{min}_{t'\,.\,t \to t'}\; d(s',t') \leq d(s,t)$

$$pd(s,t) \;\sqcup\; \mathbf{max}_{s'\,.\,s \to s'}\; \mathbf{min}_{t'\,.\,t \to t'}\; d(s',t') \leq d(s,t)$$

$$bd^{<} = \mu D \,.\, pd(s,t) \;\sqcup\; \mathbf{max}_{s'\,.\,s \to s'}\; \mathbf{min}_{t'\,.\,t \to t'}\; D(s',t')$$

this gives fix point algorithm

Bisimulation Distance

simulation distance

$$bd^{<} = \mu D \,.\, pd(s,t) \;\sqcup\; \mathbf{max}_{\,s' .\, s \to s'} \;\mathbf{min}_{\,t' .\, t \to t'}\; D(s',t')$$

bisimulation: symmetric version of simulation

$$\begin{aligned} bd^{=} = \mu D \,.\, pd(s,t) \;&\sqcup\; \mathbf{max}_{\,s' .\, s \to s'} \;\mathbf{min}_{\,t' .\, t \to t'}\; D(s',t') \\ &\sqcup\; \mathbf{max}_{\,t' .\, t \to t'} \;\mathbf{min}_{\,s' .\, s \to s'}\; D(s',t') \end{aligned}$$

Quantitative Computation Tree Logic (QCTL)

- (minimal) syntax

$$\Phi := p \mid \Phi \vee \Phi \mid \neg \Phi \mid \exists \Psi \mid \Phi \oplus c$$

$c \in [0,1]$

$$\Psi := \neg \Psi \mid \Diamond \Phi \mid \bigcirc \Phi$$

- semantics

In papers: $Q\mu$ calculus

$$[\![p]\!](s) = s(p)$$

$$[\![\neg \Phi]\!](s) = 1 - [\![\Phi]\!](s)$$

$$[\![\Phi_1 \vee \Phi_2]\!](s) = \max([\![\Phi_1]\!](s) , [\![\Phi_2]\!](s))$$

$$[\![\Phi \oplus c]\!](s) = \max([\![\Phi]\!](s) + c, 1)$$

$$[\![\Diamond \Phi]\!](\sigma) = \sup_i [\![\Phi]\!](\sigma^i)$$

$$[\![\bigcirc \Phi]\!](\sigma) = [\![\Phi]\!](\sigma^1)$$

$$[\![\exists \Psi]\!](s) = \sup_{\sigma \in \text{traces}(s)} [\![\Psi]\!](\sigma)$$

Branching Characterization Results

- boolean:

  $A \equiv_{bis} B$ iff $\forall \phi \in CTL.\ A \models \phi \Leftrightarrow B \models \phi$

  $A \sqsubseteq_{sim} B$ iff $\forall \phi \in CTL^{+}.\ A \models \phi \Rightarrow B \models \phi$

- quantitative:

  $bd^{=}(A, B) = \sup_{\Phi \in QCTL}.\ | [\![A]\!](\phi) - [\![B]\!](\phi) |$

  $bd^{<}(A, B) = \sup_{\Phi \in QCTL^{+}}.\ [\![A]\!](\phi) - [\![B]\!](\phi)$

$\oplus$ needed in Q-logics

Linear *versus* branching distances

- boolean:

$$A \equiv_{bis} B \quad \Rightarrow \quad A \equiv_{tr} B$$

$$\Leftarrow$$

B deterministic

- quantitative:

$$bd^{=}(A, B) \quad \geq \quad ld^{=}(A,B)$$

$$\neq$$

B deterministic

small branching distance $\Rightarrow$ small linear distance

Summary

- Quantative logics QLTL, QCTL
  - $s \models \phi \rightsquigarrow [\![\phi]\!](s) \in [0,1]$ how true is ϕ in s?
- Quantitative system relations
  - linear distances (trace inclusion/equivalence)
    - $s \equiv_{tr} t \rightsquigarrow ld(s,t)$ how similar are traces of s,t?
    - $s \subseteq_{tr} t \rightsquigarrow ld(s,t)$ how well can t match traces s?
    - characterized by QLTL
  - branching distances (bisimulation/simulation)
    - $s \equiv_{bis} t \rightsquigarrow ld(s,t)$ how bisimilar are s,t?
    - $s \subseteq_{sim} t \rightsquigarrow ld(s,t)$ how well can steps of t match steps of s?
    - characterized by QCTL

Rest of the talk

- QTSs
  1. linear setting
     - linear distance ld
     - QLTL
  2. branching setting
     - branching distance bd
     - QCTL
- Stochastic Games
  3. branching setting
     - a priori distance
     - a posteriori distance
     - Qμ-calculus
- Conclusions

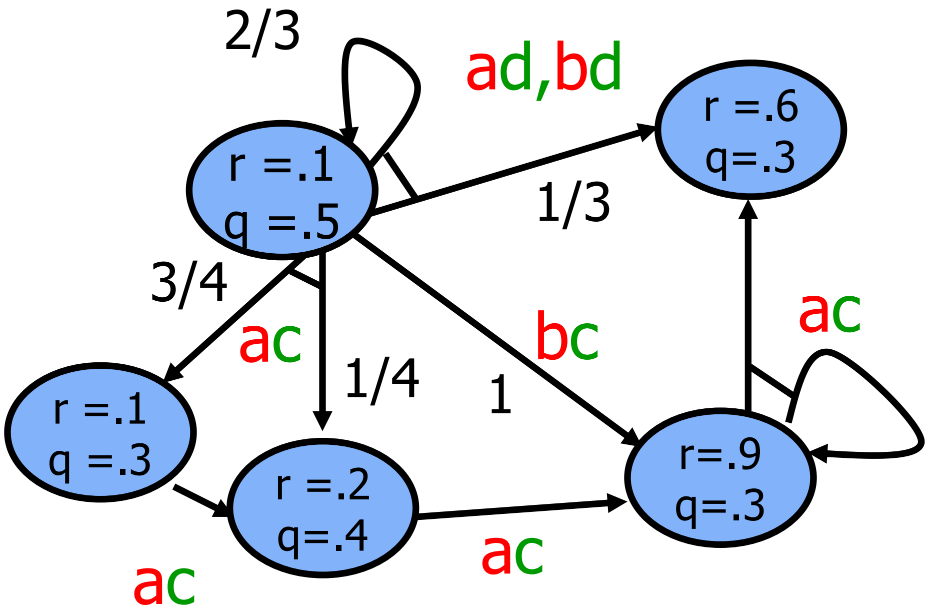
Rest of the talk

Stochastic Games

- 2 metrics
  - a posteriori distance:
  - a priori distance:

- Properties
  - coincide on MDPs, not in games
  - a priori is canocical
    - characterizes $Q\mu$
    - reciprocal = independent of the player

Stochastic concurrent 2-player games



Game model:

- repetitive games on game graph
- Two players concurrently choose their moves
  - Pl-1: **a, b**
  - Pl-2: **c, d**
- successor state is chosen probabilistically

We do not care about move names, only about reward values

Quantitative props = rewards

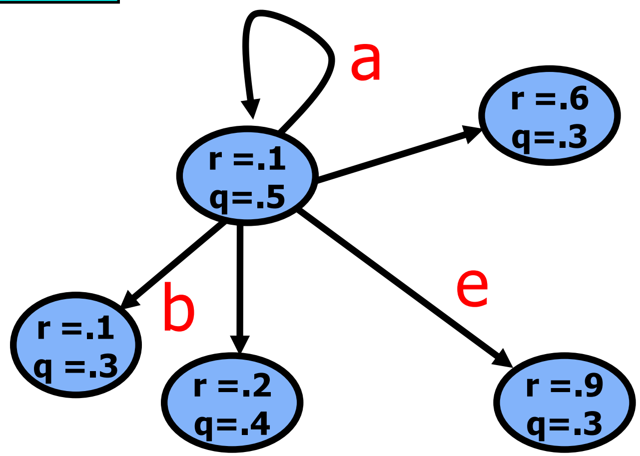
- Typical questions:
  - What is the (expected) reward player 1 is guaranteed to reach ?
  - Which minimal reward can Pl 1 maintain inf often?
  - etc

Special cases

Single player

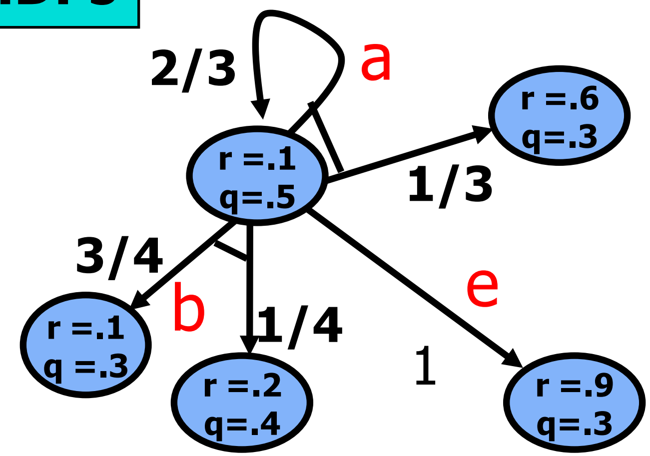
Deterministic

LTSs



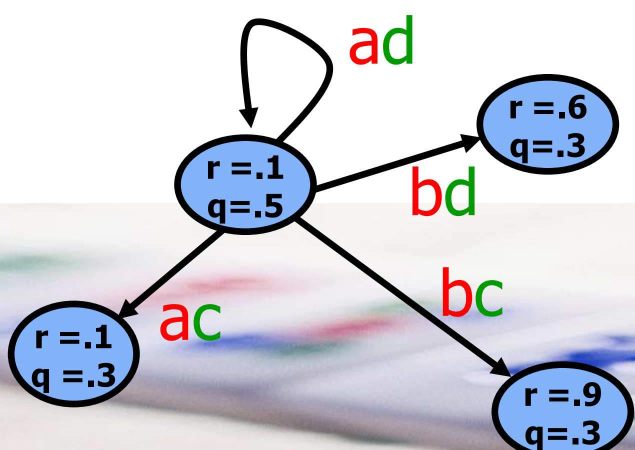
Probabilistic

MDPs

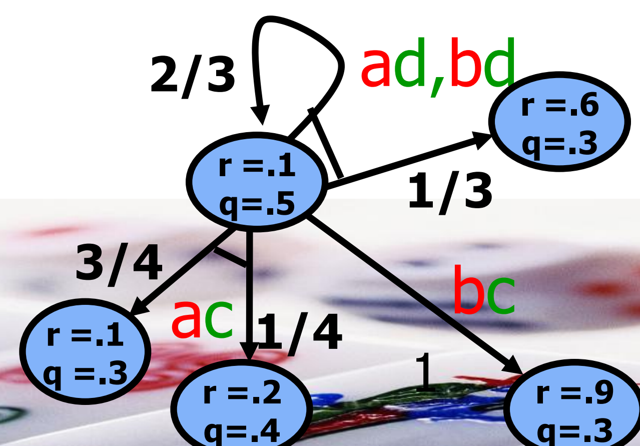


2 player

Det Games

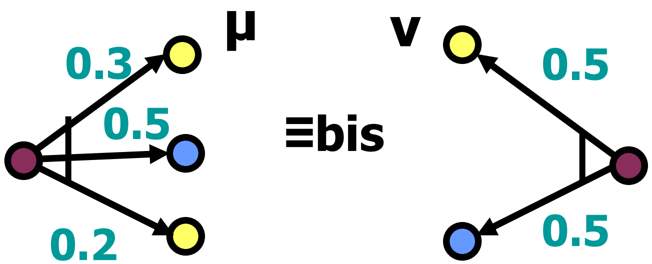


Stoch Games



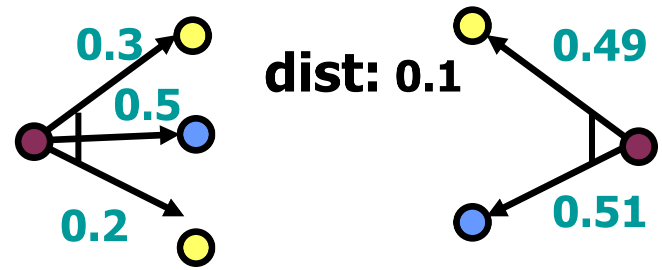
MDPs: bisimulation distance

Similarity on MDPs



$(\mu, \nu) \in R$

Simulation distance: **d(s,t)**



$\mathbf{d(\mu, \nu) \leq x}$

Relation R is a sim iff $\forall (s,t) \in R$

1. $\text{prop}(s) = \text{prop}(t)$
2. $s \rightarrow \boldsymbol{\mu}$
   $\exists \boldsymbol{\nu} \,.\, t \rightarrow \boldsymbol{\nu}$ & $(\boldsymbol{\mu}, \boldsymbol{\nu}) \in R$

$\longrightarrow$ preserves R

d is sim distance iff for all $d(s,t) = x$

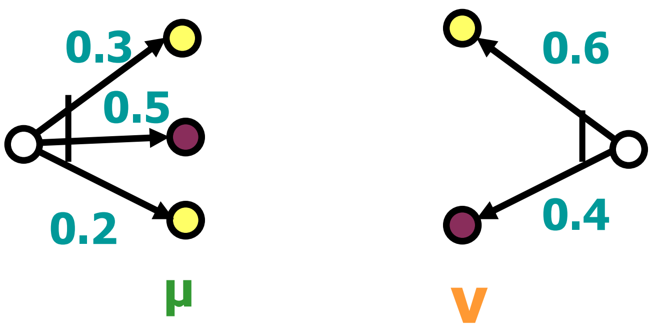
1. $d(s,t) \geq pd(s,t)$
2. $s \rightarrow \boldsymbol{\mu}$
   $\exists \boldsymbol{\nu} \,.\, t \rightarrow \boldsymbol{\nu}$ & $d(\boldsymbol{\mu}, \boldsymbol{\nu}) \leq \mathbf{x}$

$\longrightarrow$ preserves d

$bd = \mu D \,.\, pd(s,t) \sqcup \; \mathbf{max}_{\mathbf{s'} \,.\, \mathbf{s} \rightarrow \boldsymbol{\mu}} \; \mathbf{min}_{\mathbf{t'} \,.\, \mathbf{t} \rightarrow \boldsymbol{\nu}} D(\mu, \nu)$

Distance between distributions

distribution distance: **d(μ,ν)**



d(,) = 0.2

d(μ,ν) = ??

bd = μ D . pd(s,t) ⊔

max $_{s'.s\to\mu}$ **min** $_{t'.t\to\nu}$ **D(μ, ν)**

= μ D . pd(s,t) ⊔

max $_{s'.s\to\mu}$ **min** $_{t'.t\to\nu}$

max$_k$ Eμ[k] - Eν[k]

A posteriori distance

- max difference in rewards

k( ) = 0 k( ) = 0.2

Eμ[k] = 0.5*0.2 = 0.1

Eν[k] = 0.4*0.2 = 0.08

Eμ [k] - Eν[k] = 0.02

- maximize over k

$$\max_{k} \quad E\mu[k] - E\nu[k]$$

k(s) – k(t)≤ d(s,t)

$$\boxed{d(\mu,\nu) = \max_k \quad E\mu[k] - E\nu[k]}$$

A posteriori and *a priori* distances

A posteriori distance

$d_{\mathbf{post}} = \mu D \,.\, pd(s,t) \sqcup \quad \mathbf{max}_{\mathbf{s\,.\,s\to\mu}} \ \mathbf{min}_{\mathbf{t\,.\,t\to v}} \ \mathbf{max}_{\mathbf{k}} \ E\mu[k] - Ev[k]$

A priori distance

$d_{\mathbf{prio}} = \mu D \,.\, pd(s,t) \sqcup \quad \mathbf{max}_{\mathbf{k}} \ \mathbf{max}_{\mathbf{s\,.\,s\to\mu}} \ \mathbf{min}_{\mathbf{t\,.\,t\to v}} \ E\mu[k] - Ev[k]$

best match $\mathbf{t} \to \mathbf{v}$
depends on current
goal k

MDPs: *a priori* and *a posteriori* coincide

$d_{\mathbf{prio}} =$

$\mu D\ .pd(s,t) \sqcup \max_k \quad \max_{s \to \mu} \min_{t \to v} E\mu[k] - Ev[k] =$

$\mu D\ .pd(s,t) \sqcup \max_{s \to \mu} \max_k \quad \min_{t \to v} E\mu[k] - Ev[k] =$

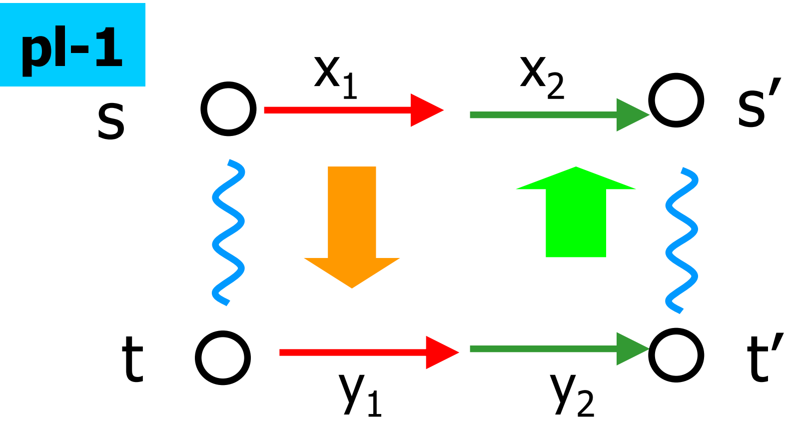
$\mu D\ .pd(s,t) \sqcup \max_{s \to \mu} \min_{t \to v} \max_k \quad E\mu[k] - Ev[k] =$

$d_{\mathbf{post}}$

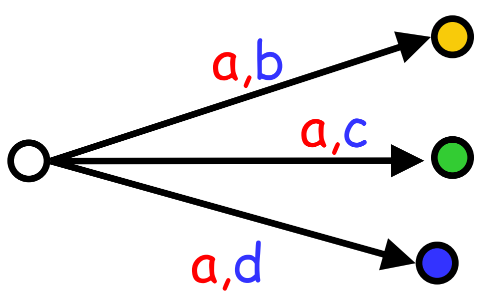
by minimax

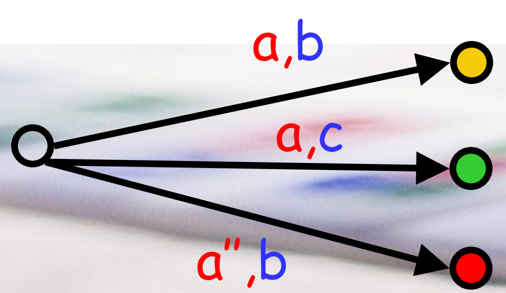
Games: a posteriori distance

Game/alternating similarity: $s \sqsubseteq_{alt} t$



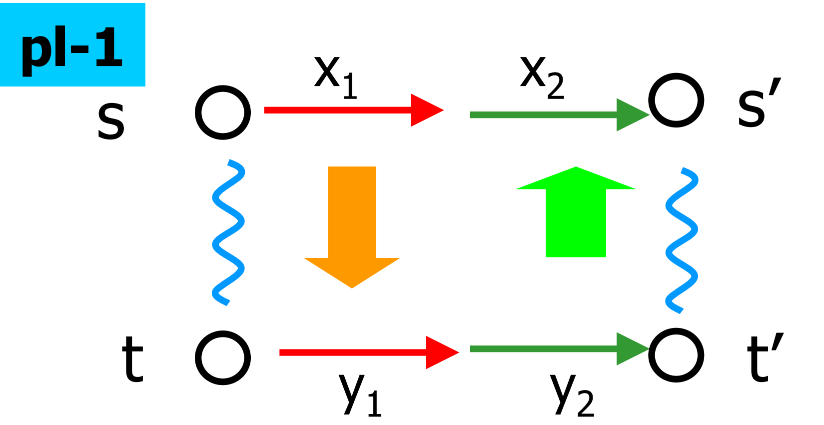
- Move y_1 is at least as good as x_1
- If x_1 wins, then y_1 wins
- Whatever bad move the opponent has in t, I have an equally bad move in s
- Hence: if I win in s, I win in t





Games: a posteriori distance

Alternating bisimilarity: $s \equiv_{alt} t$



- Move y_1 is at least as good as x_1
- If x_1 wins, then y_1 wins
- Whatever bad move the opponent has in t′ I have an equally bad move in s
- Hence: if I win in s, I win in t

R is pl-1 alternating bisim

1. prop(s) = prop(t)
2. $\forall\, x_1\, \exists\, y_1\, \forall\, y_2\, \exists\, x_2.$

   for $s \rightarrow s'$, $t \rightarrow t'$
   $(s',t') \in R$

Metric d is a priori distance

1. $d(s,t) \leq ld(s,t)$
2. **max x_1 min y_1 max y_2 min x_2.** $d(\mu,\nu)$ =

= **max x_1 min y_1 max y_2 min x_2. $\max_k$**

$E_{x1x2}[k] - E_{y1y2}[k]$

Games: *a priori* vs *a posteriori* metrics

$$\mathbf{d_{post}} = \mu D\ .pd(s,t) \sqcup$$
$$\max x_1 \min y_1 \max y_2 \min x_2.\ \max_k \mathbf{E_{x1x2}}[k] - \mathbf{E_{y1y2}}[k]$$

$$\mathbf{d_{prio}} = \mu D\ .pd(s,t) \sqcup$$
$$\max_k \max x_1 \min y_1 \max y_2 \min x_2.\ \mathbf{E_{x1x2}}[k] - \mathbf{E_{y1y2}}[k]$$

$$\begin{aligned}
& \max_k \max_{x_1} \min_{x_2} \max_{y_2} \min_{y_1} E^{x_1,x_2}(k) - E^{y_1,y_2}(k) \\
= \ & \max_{x_1} \max_k \min_{x_2} \max_{y_2} \min_{y_1} E^{x_1,x_2}(k) - E^{y_1,y_2}(k) \\
\leqslant \ & \max_{x_1} \min_{x_2} \max_k \max_{y_2} \min_{y_1} E^{x_1,x_2}(k) - E^{y_1,y_2}(k) \\
= \ & \max_{x_1} \min_{x_2} \max_{y_2} \max_k \min_{y_1} E^{x_1,x_2}(k) - E^{y_1,y_2}(k) \\
= \ & \max_{x_1} \min_{x_2} \max_{y_2} \min_{y_1} \max_k E^{x_1,x_2}(k) - E^{y_1,y_2}(k)
\end{aligned}$$

Hence: $\mathbf{d_{prio}} \leq \mathbf{d_{post}}$

Reciprocity of a priori metric

PL-1

$bd_{prio} = \mu D \,.\, pd(s,t)$

$\max_k \; \max_{x1} \min_{x2} \max_{y1} \min_{y2} E_{x1x2}[k] - E_{y1y2}[k]$

$= \mu D \,.\, pd(s,t)$

$\max_k \; \max_{x1} \min_{x2} E_{x1x2}[k] - \max_{y1} \min_{y2} E_{y1y2}[k]$

determinacy of stoch games

$= \mu D \,.\, pd(s,t)$

$\max_k \; \min_{x2} \max_{x1} E_{x1x2}[k] - \min_{y2} \max_{y1} E_{y1y2}[k]$

push though minus

$= \mu D \,.\, pd(s,t)$

$\max_k \; \max_{y2} \min_{y1} E_{y1y2}[k] - \max_{x1} \min_{x2} E_{y1y2}[k]$

PL-2

$Q\mu$ Quantitative μCalculus

- syntax

$$\Phi := R \mid \Phi \vee \Phi \mid \neg\Phi \mid Z \mid \mathrm{Pre}_i(\Phi) \mid \Phi \oplus c \mid \mu Z.\ \Phi$$

- semantics

$$[\![R]\!](s) = s(R)$$

$$[\![\neg \Phi]\!](s) = 1 - [\![\Phi]\!](s)$$

$$[\![\Phi_1 \vee \Phi_2]\!](s) = \max([\![\Phi_1]\!](s), [\![\Phi_2]\!](s))$$

$$[\![\Phi \oplus c]\!](s) = \max([\![\Phi]\!](s) + c, 1)$$

$[\![\mathrm{Pre}_i\ \Phi]\!](\sigma)$ = maximal reward player i can enforce in single step, for rewards given by Φ

Branching Characterization Results

- *a priori* distance characterizes Qμ:

$$bd_{\mathbf{prio}}(A, B) \quad = \quad \sup_{\Phi \in \mathrm{Qmu}}{}^{+}. \ \ [\![A]\!](\phi) \ - \ [\![B]\!](\phi)$$

(similarly for symmetric variant)

- no characterization for $bd_{\mathbf{prio}}$

Outline of this talk

Stochastic Games

- 2 metrics
  - a posteriori distance:
  - a priori distance:

- Properties
  - coincide on MDPs, not in games
  - a priori is canocical
    - characterizes $Q\mu$
    - reciprocal = independent of the player

References

- **Game Relations and Metrics.**
  L. de Alfaro, R. Majumdar, V. Raman, M.I.A Stoelinga.
  Proceedings of LICS'07
- **Model checking Quantitative Linear Time Logic**
  M. Faella, A. Legay, M.I.A. Stoelinga
  Proceedings of QAPL'08
- **Linear and Branching Metrics for Quantitative Transition Systems.**
  L. de Alfaro, M. Faella, M.I.A. Stoelinga.
  In *Proceedings of ICALP'04.* Submitted to LMCS.
- **Model Checking Discounted Temporal Properties.**
  L. de Alfaro, M. Faella, T.A. Henzinger, R. Majumdar,
  M.I.A. Stoelinga.
  In *J. of Theoretical Computer Science'05*