



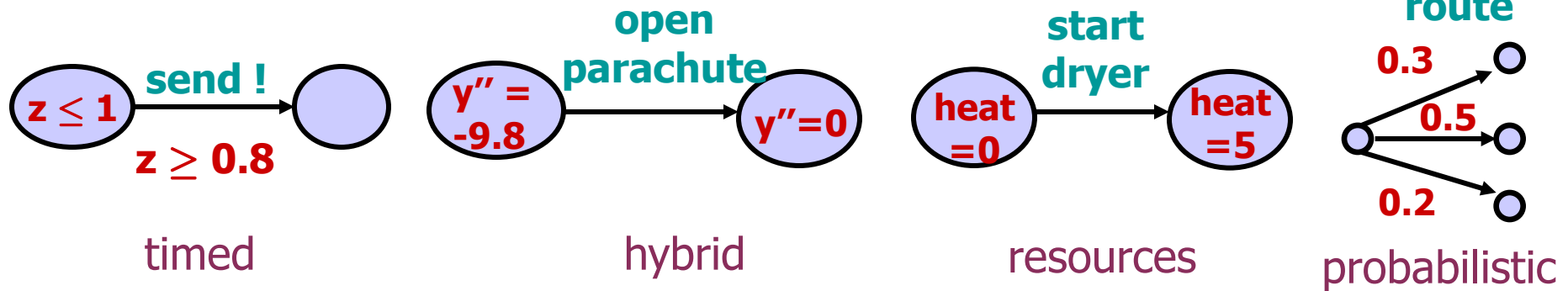
From Quality to Quantity:

Logics and Metrics for
Quantitative System
models

Marielle Stoelinga
University of Twente

From Quality to Quantity

Quantitative system models

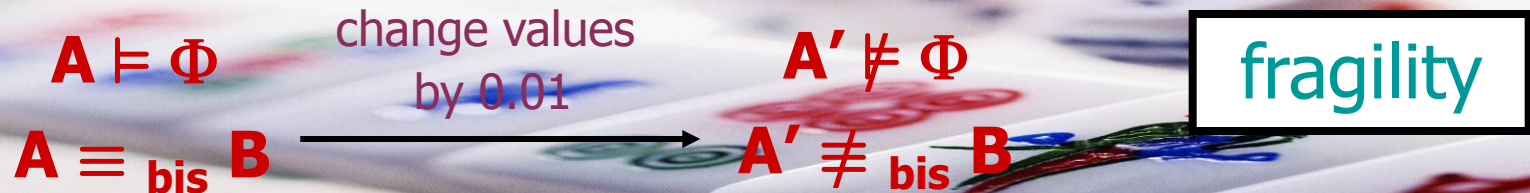


Verification is usually boolean:

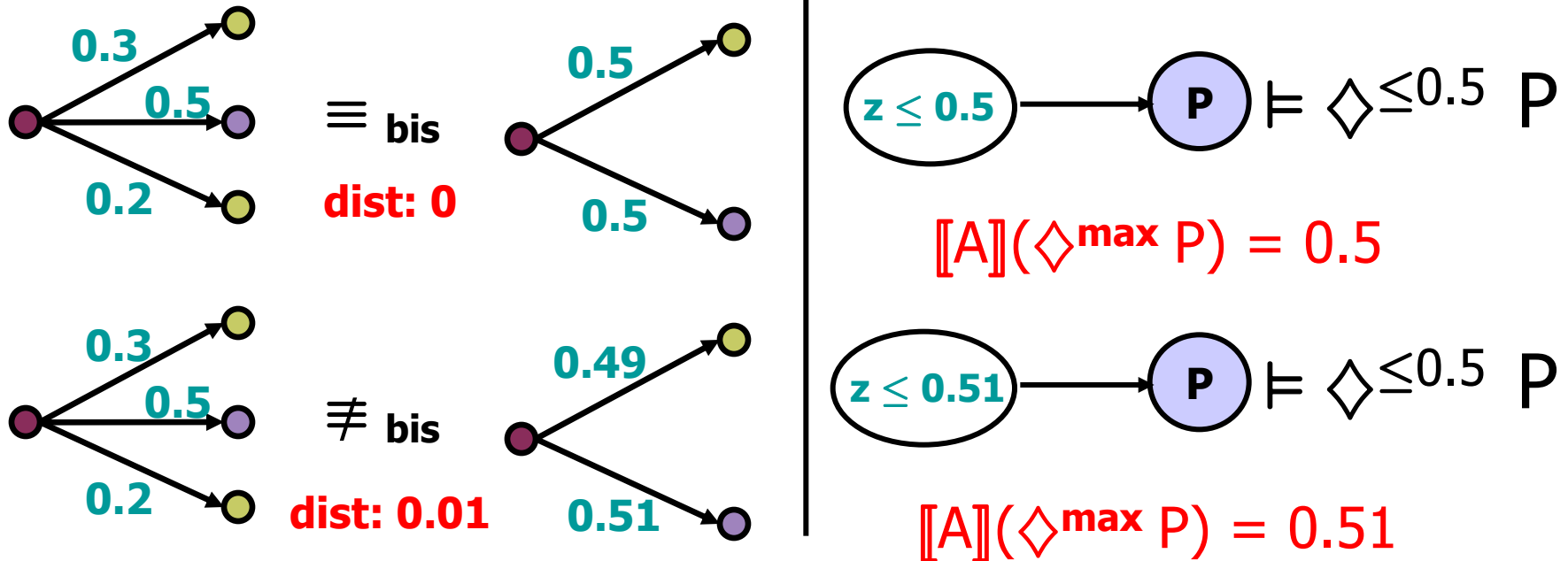
- either $\mathbf{A} \models \Phi$ or $\mathbf{A} \not\models \Phi$
- either $\mathbf{A} \equiv_{\text{bis}} \mathbf{B}$ or $\mathbf{A} \not\equiv_{\text{bis}} \mathbf{B}$

Problem:

- lack of expressiveness: quantify our satisfaction
- small perturbations have large effects



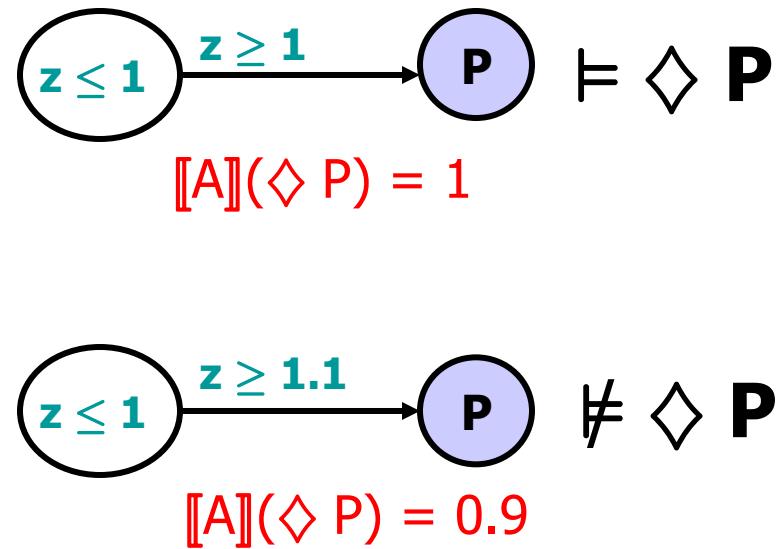
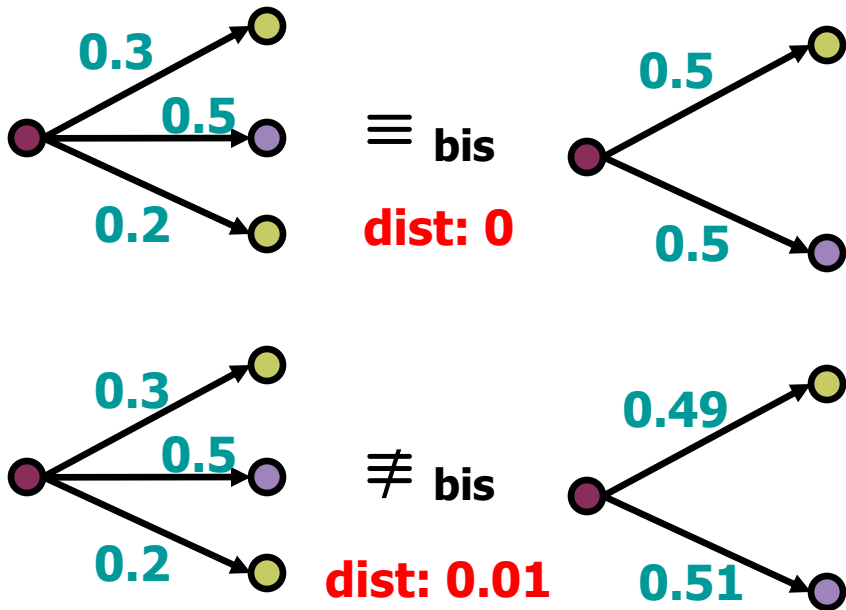
From Quality to Quantity



Our opinion: verification should be **quantitative**

- $A \models \phi \rightsquigarrow \llbracket A \rrbracket (\phi) \in [0,1]$ how true is ϕ on **A**?
- $A \equiv_{\text{bis}} B \rightsquigarrow \text{dist}(A,B)$ how similar are A and B?
distance/metric

From Quality to Quantity



Quantitative system relations

$\square s \sqsubseteq t \rightsquigarrow \text{dist}(s,t)$

how similar are two systems?

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

Quantitative logics

$\square s \models \phi \rightsquigarrow \llbracket \phi \rrbracket(s) \in [0,1]$

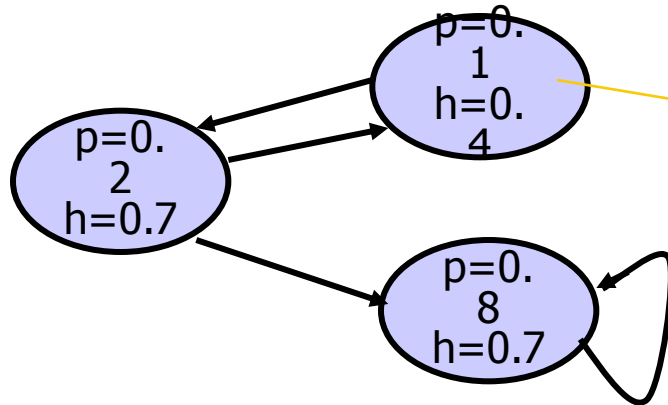
how true is ϕ in s ?

- Quantitative LTL
- Quantitative CTL

The model

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

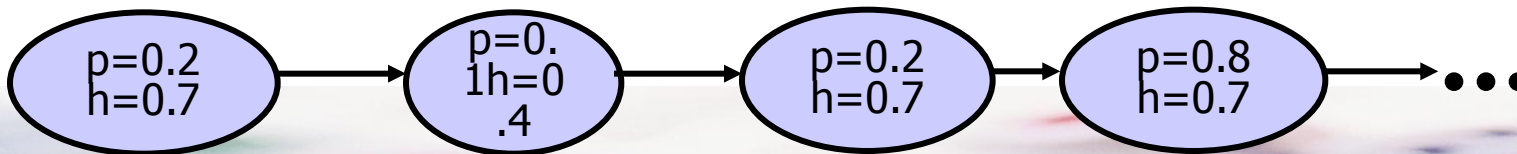
- **Quantitative Transition Systems (QTSs)**
kripke structures with quantitative predicates



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

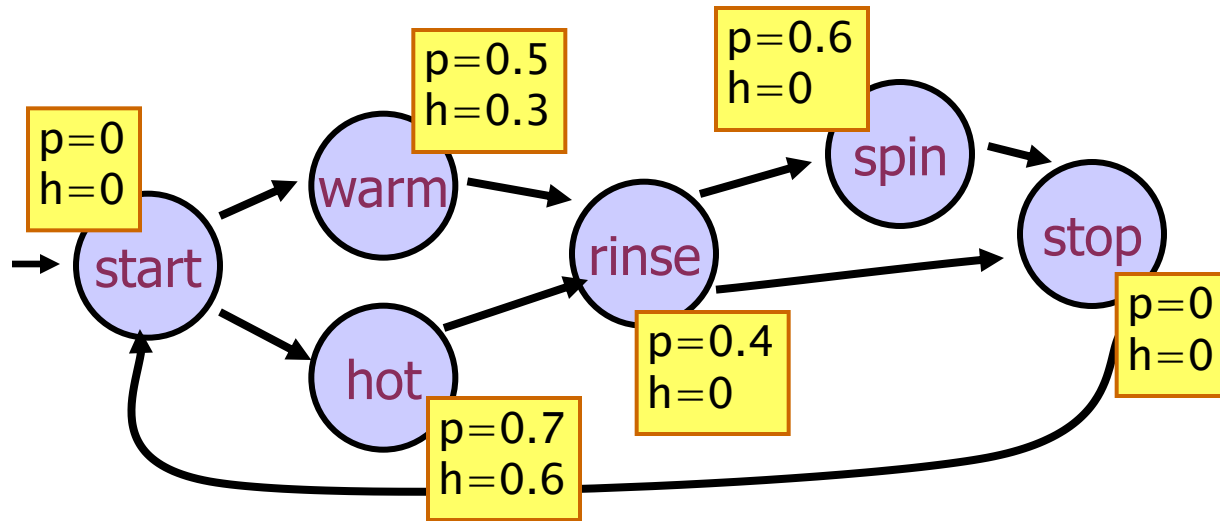
express: priorities, fuzzy predicates, rewards, power, heat,

- **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

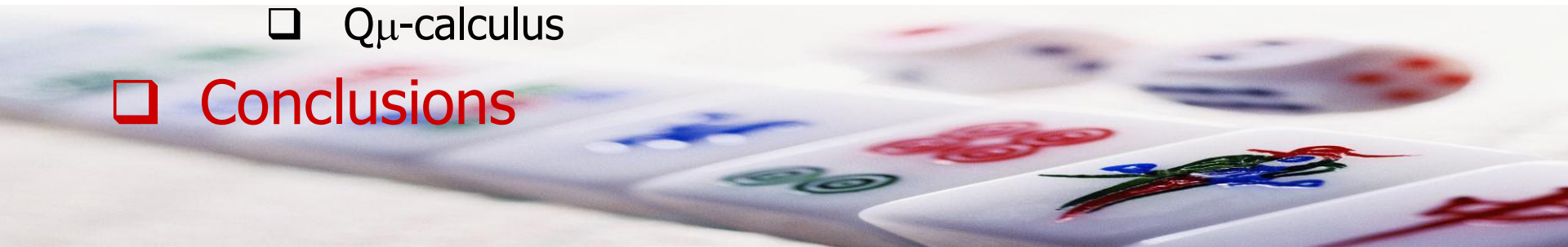
- branching distance bd
- QCTL

□ Stochastic Games

3. branching setting

- a priori distance
- a posteriori distance
- $Q\mu$ -calculus

□ Conclusions



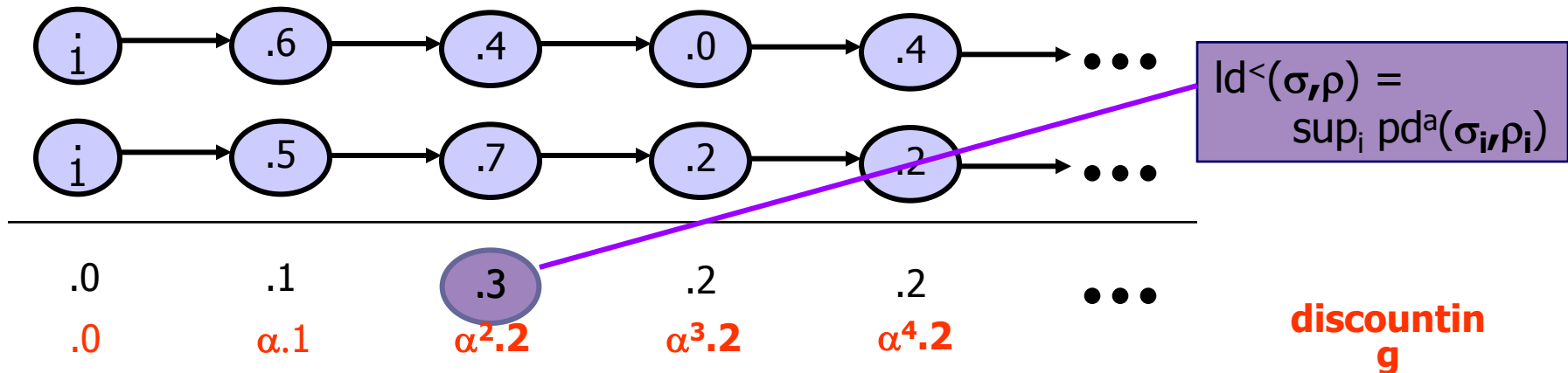
Linear Distances (trace inclusion/equivalence)

- How different are two states? *Propositional distance*

$$\text{pd}\left(\begin{array}{c} p=0.1 \\ q=0.8 \end{array}, \begin{array}{c} p=0.3 \\ q=0.7 \end{array} \right) = 0.2$$

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

- How different are two traces? *Trace distance*



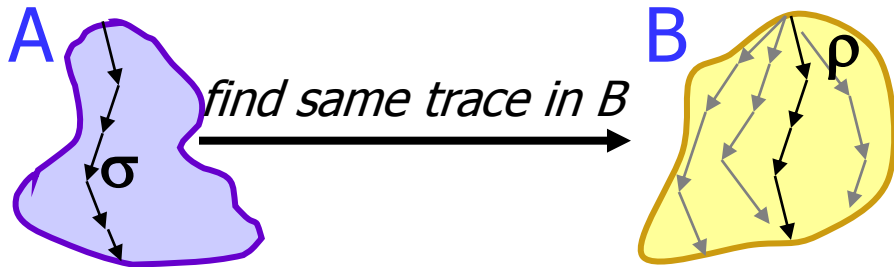
- How different are two systems? *Hausdorff set distance*

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

.... see next slide

Linear Distances

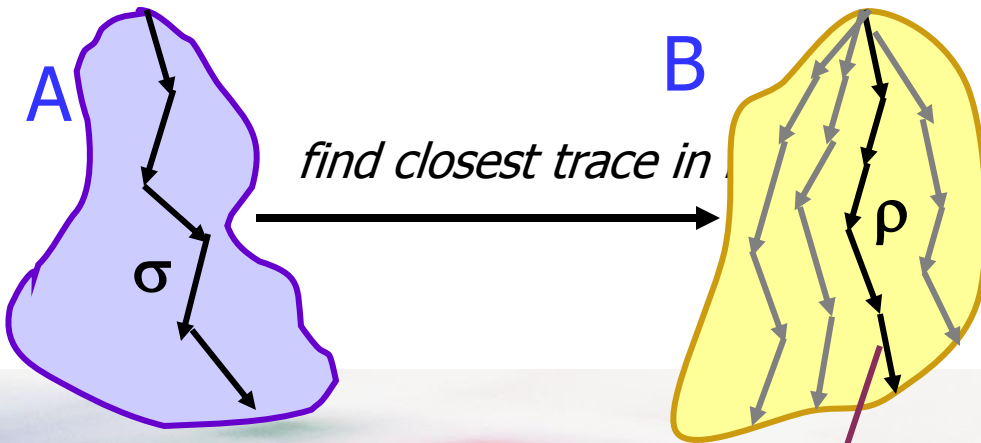
Trace inclusion: $A \sqsubseteq_{\text{tr}} B = \text{tr}(A) \subseteq \text{tr}(B)$



$$A \sqsubseteq_{\text{tr}} B = \forall \sigma \in \text{tr}(A) \exists \rho \in \text{tr}(B). \sigma = \rho$$

$$A =_{\text{tr}} B = A \sqsubseteq_{\text{tr}} B \ \& \ B \sqsubseteq_{\text{tr}} A$$

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



Find hardest trace in A to match

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

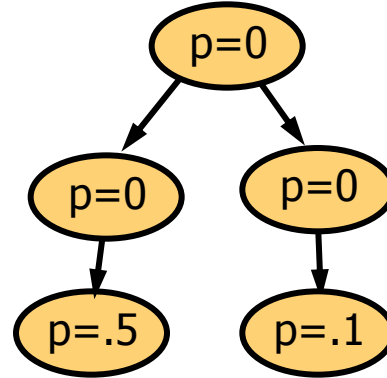
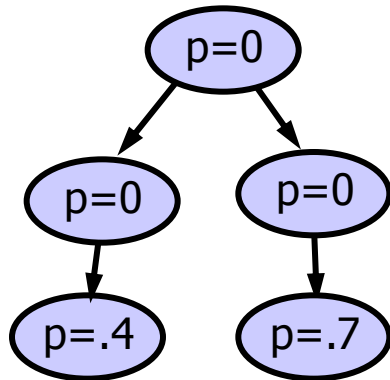
symmetric variant

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

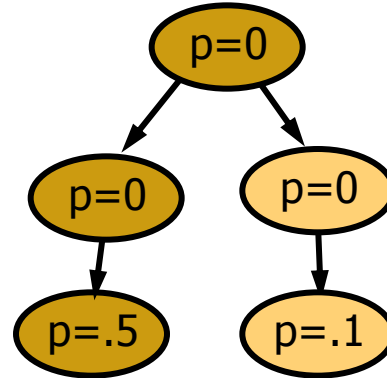
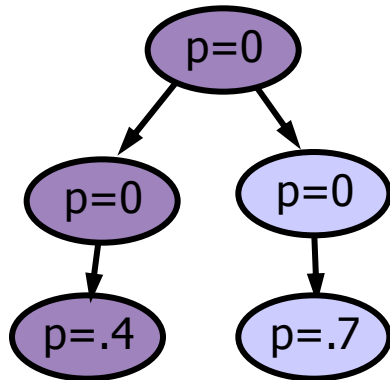
= trace at min dist

$$= \inf_{\rho \in \text{tr}(B)} \text{ld}^<(\sigma, \rho)$$

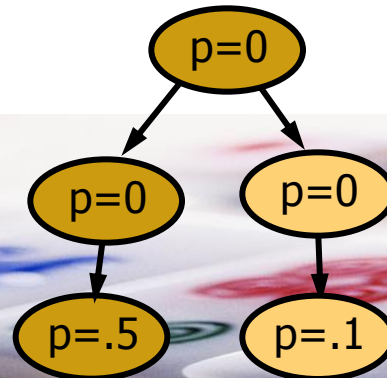
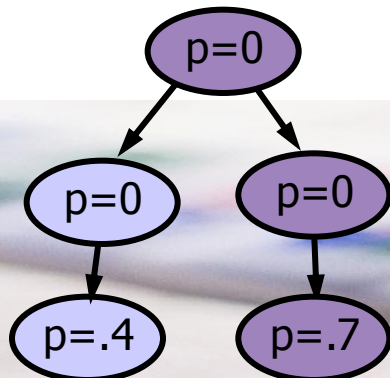
Ld<(A,B): example



dist: .2



dist: .1



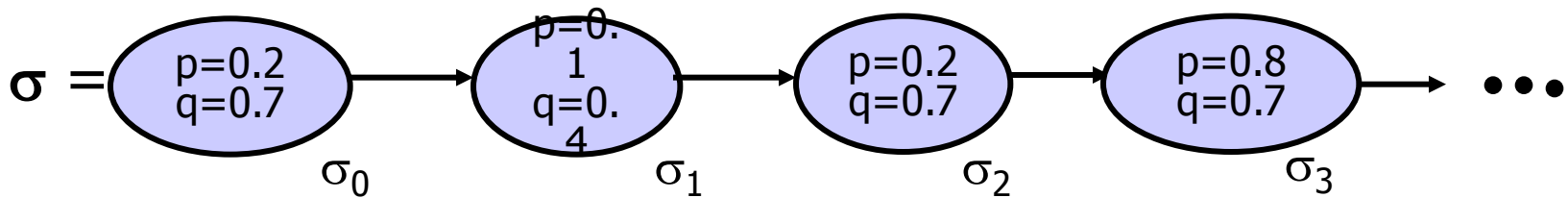
dist: .2

Quantitative Linear Time Logic (QLTL)

□ (minimal) syntax

$\Phi := p \mid \Phi \vee \Phi \mid \neg \Phi \mid \bigcirc \Phi \mid \diamond \Phi \mid \Phi \oplus c \quad c \in [0,1]$

□ semantics



□ $[[p]](\sigma) = \sigma_0(p)$

□ $[[\neg \Phi]](\sigma) = 1 - [[\Phi]](\sigma)$

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

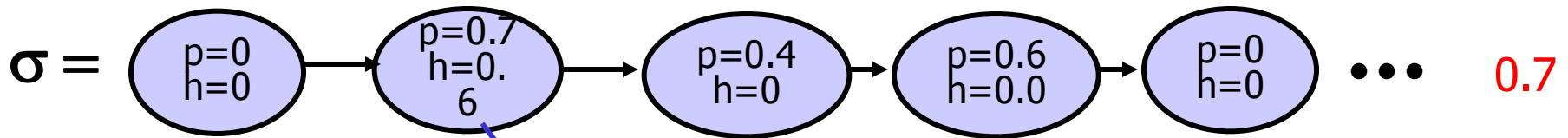
□ $[[\Phi_1 \vee \Phi_2]](\sigma) = \max([[\Phi_1]](\sigma), [[\Phi_2]](\sigma))$

□ $[[\diamond \Phi]](\sigma) = \sup_i [[\Phi]](\sigma^i)$

□ $[[\Phi \oplus c]](\sigma) = \min([[\Phi]](\sigma) + c, 1)$

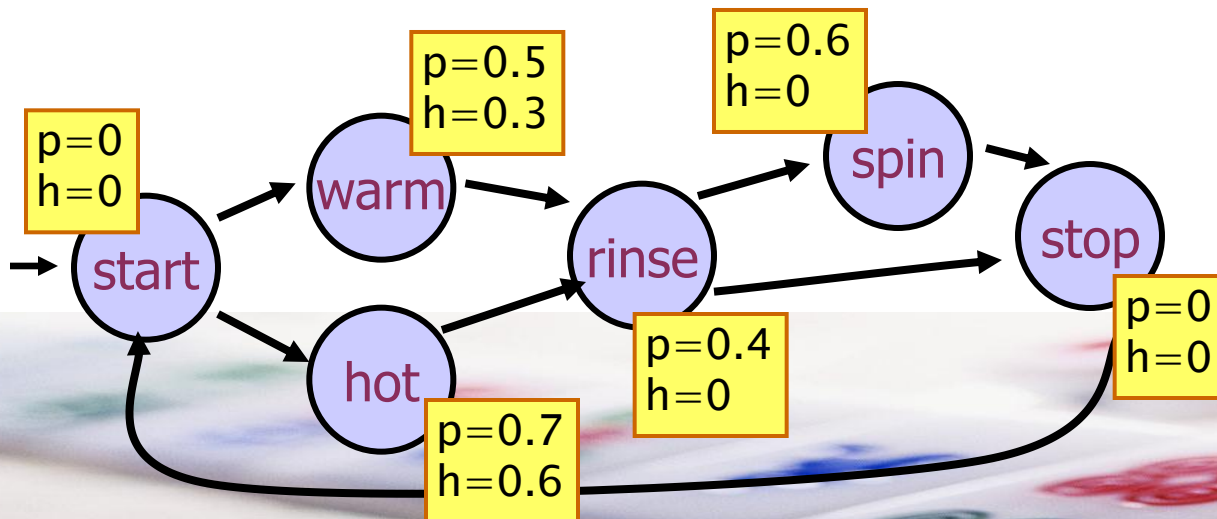
$[[\Phi]](s) = \inf_{\sigma \in \text{tr}(s)} [[\Phi]](\sigma)$

Semantics for $\diamond p$



$$[\diamond p](\sigma) = \sup_i (\sigma^i)(p) = 0.7$$

Washing Machine



$$[\diamond p](s) = \inf_{\sigma} [\diamond p](\sigma) = 0.6$$

$\diamond p = 0.6$
min peak consumption

Linear Characterization Results

□ boolean:

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

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

□ quantitative:

$$\text{Id}^=(A, B) = \sup_{\phi \in \text{QLTL}} | \llbracket A \rrbracket(\phi) - \llbracket B \rrbracket(\phi) |$$

$$\text{Id}^<(A, B) = \sup_{\phi \in \text{QLTL}^+} \llbracket A \rrbracket(\phi) - \llbracket B \rrbracket(\phi)$$

⊕ needed in Q-logics

Two directions:

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

Part 2: Simulation Distance

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

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

1. $\text{prop}(s) = \text{prop}(t)$
2. $s \rightarrow s' \Rightarrow \exists t'. t \rightarrow t' \ \& \ (s',t') \in R$

\rightarrow preserves R

\sqsubseteq_{sim} is the largest sim rel

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

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

1. $d(s,t) \geq \text{pd}(s,t)$
2. $s \rightarrow s' \Rightarrow \exists t'. t \rightarrow t' \ \& \ d(s',t') \leq x$

\rightarrow preserves d

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

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

Simulation Distance

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

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

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

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

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

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

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

this gives fix point algorithm

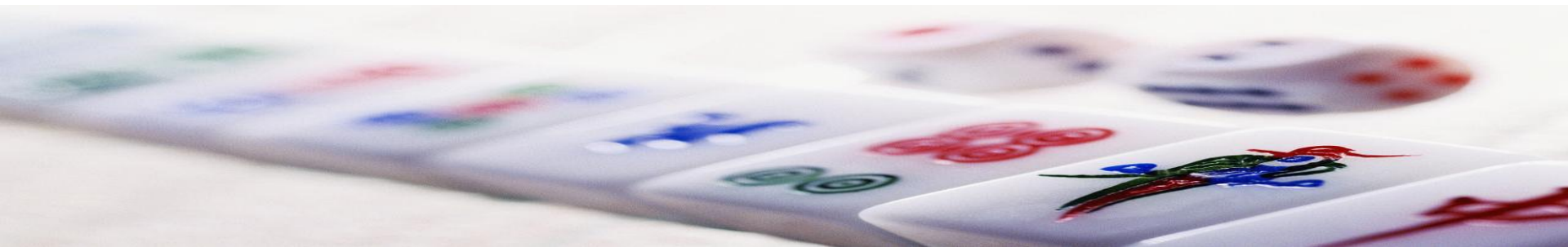
Bisimulation Distance

simulation distance

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

bisimulation: symmetric version of simulation

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



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

$$\llbracket p \rrbracket(s) = s(p)$$

$$\llbracket \neg \Phi \rrbracket(s) = 1 - \llbracket \Phi \rrbracket(s)$$

$$\llbracket \Phi_1 \vee \Phi_2 \rrbracket(s) = \max(\llbracket \Phi_1 \rrbracket(s), \llbracket \Phi_2 \rrbracket(s))$$

$$\llbracket \Phi \oplus c \rrbracket(s) = \max(\llbracket \Phi \rrbracket(s) + c, 1)$$

$$\llbracket \diamond \Phi \rrbracket(\sigma) = \sup_i \llbracket \Phi \rrbracket(\sigma^i)$$

$$\llbracket \bigcirc \Phi \rrbracket(\sigma) = \llbracket \Phi \rrbracket(\sigma^1)$$

$$\llbracket \exists \Psi \rrbracket(s) = \sup_{\sigma \in \text{traces}(s)} \llbracket \Psi \rrbracket(\sigma)$$

In papers:
 Q_μ calculus

Branching Characterization Results

□ boolean:

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

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

□ quantitative:

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

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

⊕ needed in Q-logics

Linear *versus* branching distances

□ boolean:

$$A \equiv_{\text{bis}} B \quad \begin{array}{c} \Rightarrow \\ \Leftarrow \end{array} \quad A \equiv_{\text{tr}} B$$

B deterministic

□ quantitative:

$$\text{bd}^=(A, B) \quad \begin{array}{c} \geq \\ \neq \end{array} \quad \text{ld}^=(A, B)$$

B deterministic

small branching distance \Rightarrow small linear distance



Summary

Quantitative logics QLTL, QCTL

$s \models \phi \rightsquigarrow \llbracket \phi \rrbracket(s) \in [0,1]$ how true is ϕ in s ?

Quantitative system relations

linear distances (trace inclusion/equivalence)

$s \equiv_{tr} t \rightsquigarrow \text{ld}(s,t)$ how similar are traces of s,t ?

$s \subseteq_{tr} t \rightsquigarrow \text{ld}(s,t)$ how well can t match traces s ?

characterized by QLTL

branching distances (bisimulation/simulation)

$s \equiv_{bis} t \rightsquigarrow \text{ld}(s,t)$ how bisimilar are s,t ?

$s \subseteq_{sim} t \rightsquigarrow \text{ld}(s,t)$ 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
 - $Q\mu$ -calculus

□ Conclusions



Rest of the talk

Stochastic Games

□ 2 metrics

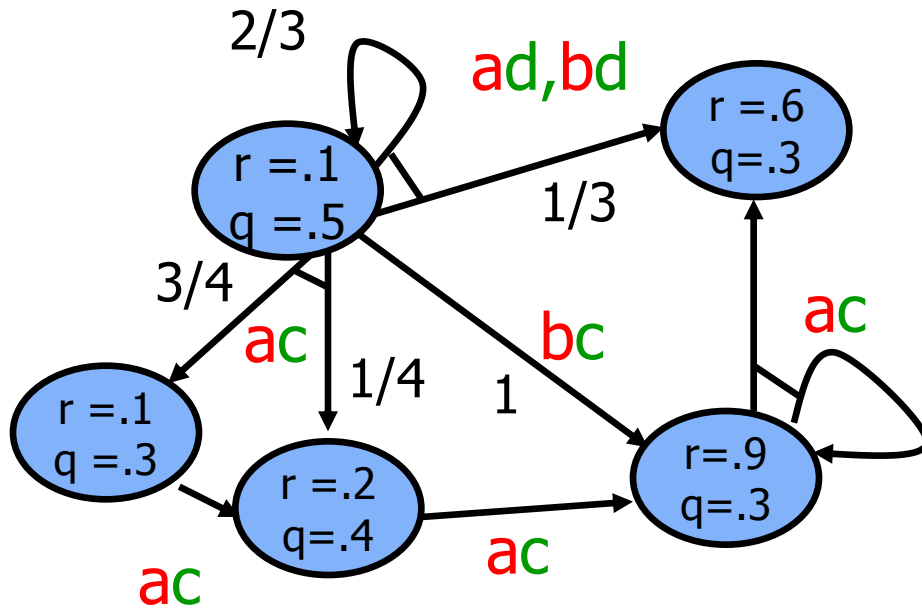
- a posteriori distance:
- a priori distance:

□ Properties

- coincide on MDPs, not in games
- a priori is canonical
 - characterizes Q_μ
 - reciprocal = independent of the player



Stochastic concurrent 2-player games



Game model:

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

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

Quantitative props = rewards

■ Typical questions:

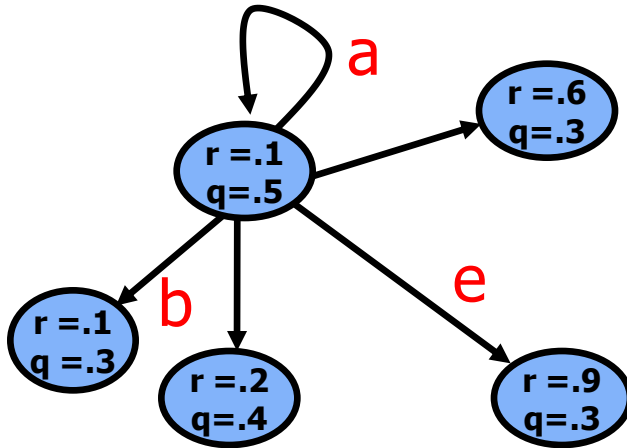
- What is the (expected) reward player 1 is guaranteed to reach ?
- Which minimal reward can PI 1 maintain inf often?
- etc

Special cases

Single player

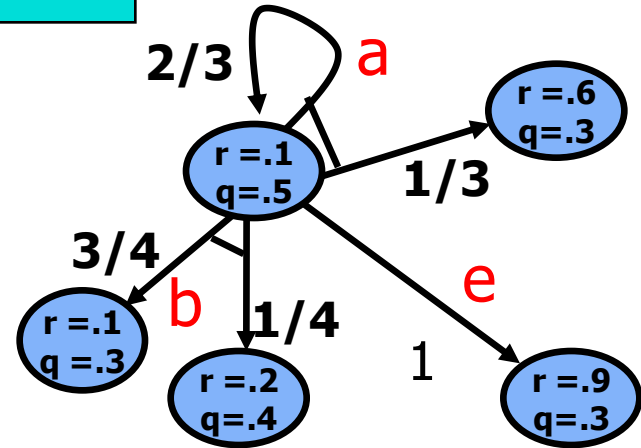
Deterministic

LTSs



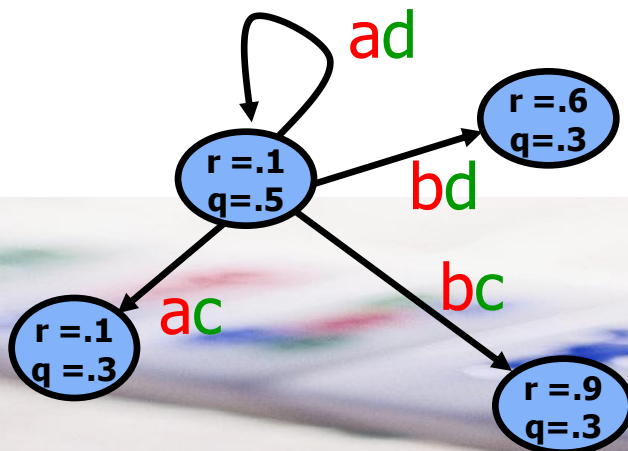
Probabilistic

MDPs

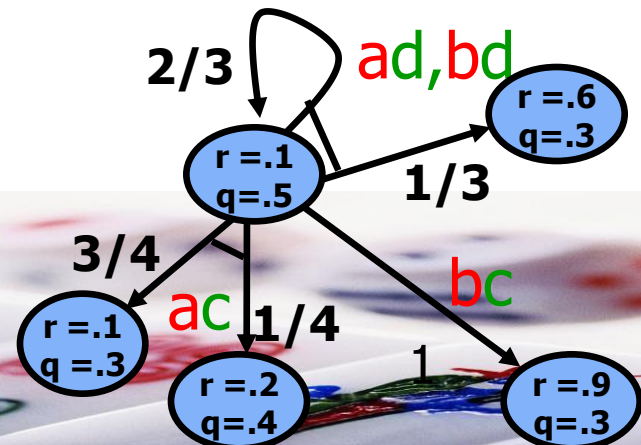


Det Games

2 player

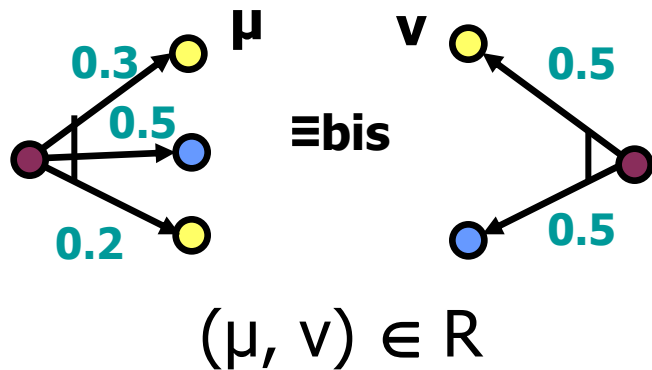


Stoch Games

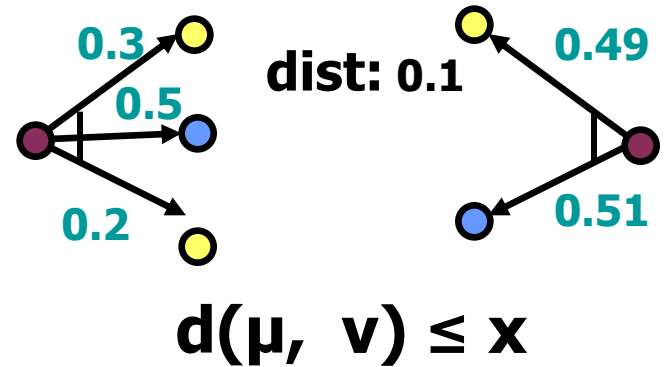


MDPs: bisimulation distance

Similarity on MDPs



Simulation distance: $d(s,t)$



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

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

\rightarrow preserves R

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

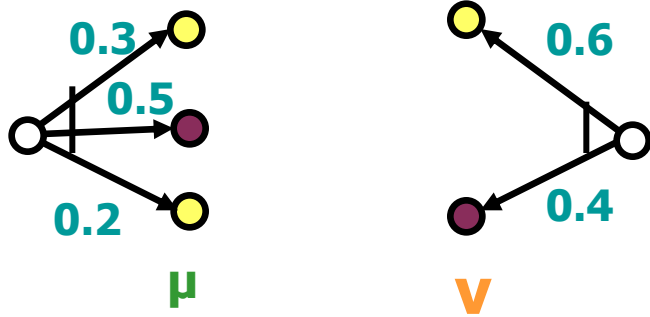
1. $d(s,t) \geq \text{pd}(s,t)$
2. $s \rightarrow \mu$
 $\exists \nu . t \rightarrow \nu \ \& \ d(\mu, \nu) \leq x$

\rightarrow preserves d

$$\text{bd} = \mu D . \text{pd}(s,t) \sqcup \max_{s' . s \rightarrow \mu} \min_{t' . t \rightarrow \nu} D(\mu, \nu)$$

Distance between distributions

distribution distance: $d(\mu, \nu)$



$$d(\text{white}, \text{purple}) = 0.2$$

$$d(\mu, \nu) = ??$$

$$\begin{aligned} \text{bd} &= \mu D \cdot \text{pd}(s, t) \sqcup \\ &\quad \max_{s' \cdot s \rightarrow \mu} \min_{t' \cdot t \rightarrow \nu} D(\mu, \nu) \\ &= \mu D \cdot \text{pd}(s, t) \sqcup \\ &\quad \max_{s' \cdot s \rightarrow \mu} \min_{t' \cdot t \rightarrow \nu} \\ &\quad \quad \max_k E\mu[k] - E\nu[k] \end{aligned}$$

A posteriori distance

- max difference in rewards

$$k(\text{white}) = 0 \quad k(\text{purple}) = 0.2$$

$$E\mu[k] = 0.5 * 0.2 = 0.1$$

$$E\nu[k] = 0.4 * 0.2 = 0.08$$

$$E\mu[k] - E\nu[k] = 0.02$$

- maximize over k

$$\max_k E\mu[k] - E\nu[k]$$

$$k(s) - k(t) \leq d(s, t)$$

$$d(\mu, \nu) = \max_k E\mu[k] - E\nu[k]$$



A posteriori and *a priori* distances

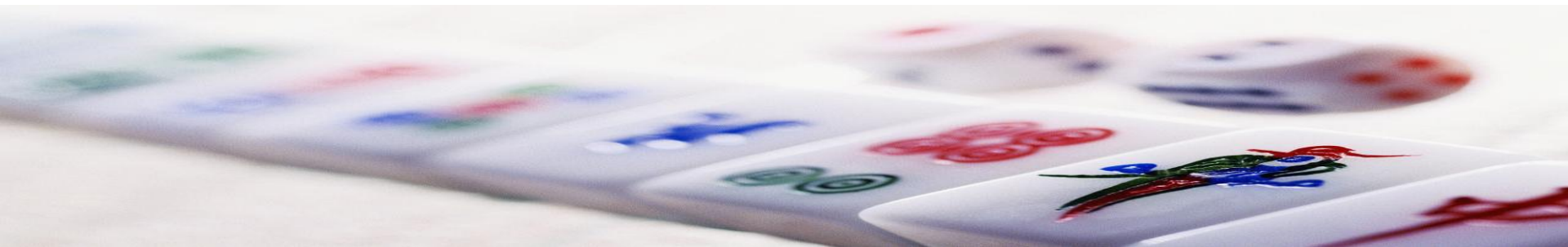
A posteriori distance

$$d_{\text{post}} = \mu D \cdot \text{pd}(s,t) \sqcup \max_{s.s \rightarrow \mu} \min_{t.t \rightarrow v} \max_k E\mu[k] - E\nu[k]$$

A priori distance

$$d_{\text{prio}} = \mu D \cdot \text{pd}(s,t) \sqcup \max_k \max_{s.s \rightarrow \mu} \min_{t.t \rightarrow v} E\mu[k] - E\nu[k]$$

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



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

$d_{\text{prio}} =$

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

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

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

d_{post}

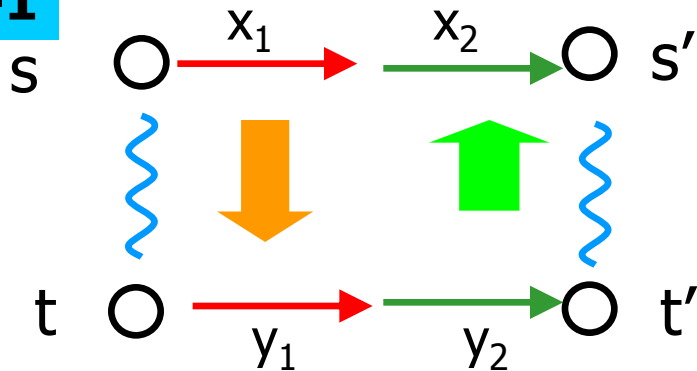
by minimax



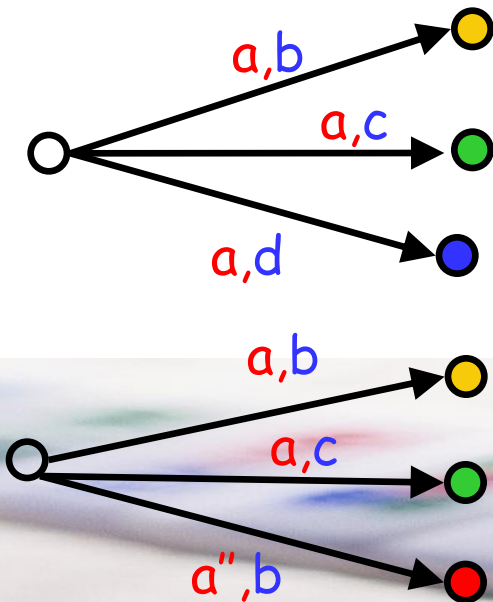
Games: a posteriori distance

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

pl-1



- 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

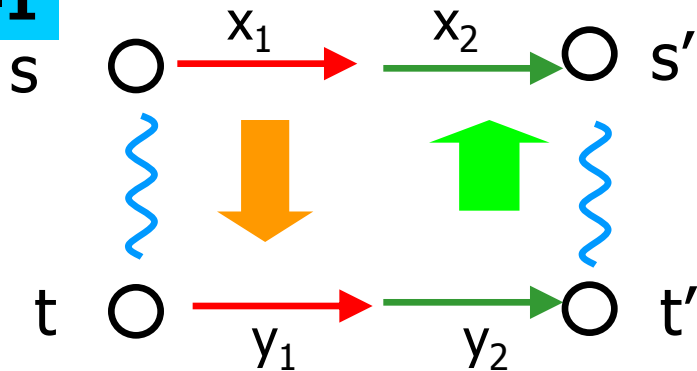


Games: a posteriori distance

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

- 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 s I have an equally bad move in t
- Hence: if I win in s , I win in t

pl-1



R is pl-1 alternating bisim

1. $\text{prop}(s) = \text{prop}(t)$

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. $d(s, t) \leq \text{ld}(s, t)$

2. $\max x_1 \min y_1 \max y_2 \min x_2. d(\mu, \nu) =$

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

$$E_{x_1 x_2} [k] - E_{y_1 y_2} [k]$$

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

$$d_{\text{post}} = \mu D .pd(s,t) \sqcup$$

$$\max_{x_1} \min_{y_1} \max_{y_2} \min_{x_2} \cdot \max_k E_{x_1 x_2}[k] - E_{y_1 y_2}[k]$$

$$d_{\text{prio}} = \mu D .pd(s,t) \sqcup$$

$$\max_k \max_{x_1} \min_{y_1} \max_{y_2} \min_{x_2} \cdot E_{x_1 x_2}[k] - E_{y_1 y_2}[k]$$

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

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

Reciprocity of a priori metric

PL-1 $bd_{prio} = \mu D \cdot pd(s,t)$

$$\max_k \max_{x_1} \min_{x_2} \max_{y_1} \min_{y_2} E_{x_1 x_2} [k] - E_{y_1 y_2} [k]$$

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

$$\max_k \max_{x_1} \min_{x_2} E_{x_1 x_2} [k] - \max_{y_1} \min_{y_2} E_{y_1 y_2} [k]$$

determinacy of stoch games

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

$$\max_k \min_{x_2} \max_{x_1} E_{x_1 x_2} [k] - \min_{y_2} \max_{y_1} E_{y_1 y_2} [k]$$

push though minus

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

$$\max_k \max_{y_2} \min_{y_1} E_{y_1 y_2} [k] - \max_{x_1} \min_{x_2} E_{y_1 y_2} [k]$$

PL-2

$Q\mu$ Quantitative μ Calculus

□ syntax

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

□ semantics

$$\llbracket R \rrbracket(s) = s(R)$$

$$\llbracket \neg \Phi \rrbracket(s) = 1 - \llbracket \Phi \rrbracket(s)$$

$$\llbracket \Phi_1 \vee \Phi_2 \rrbracket(s) = \max(\llbracket \Phi_1 \rrbracket(s), \llbracket \Phi_2 \rrbracket(s))$$

$$\llbracket \Phi \oplus c \rrbracket(s) = \max(\llbracket \Phi \rrbracket(s) + c, 1)$$

$$\llbracket \text{Pre}_i \Phi \rrbracket(\sigma) = \text{maximal reward player } i$$

can enforce in single step,
for rewards given by Φ

Branching Characterization Results

□ *a priori* distance characterizes Q_μ :

$$\text{bd}_{\text{prio}}(A, B) = \sup_{\phi \in Q_{\mu^+}} \llbracket A \rrbracket(\phi) - \llbracket B \rrbracket(\phi)$$

(similarly for symmetric variant)

□ no characterization for bd_{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 canonical
 - characterizes Q_μ
 - 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*