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

Marielle Stoelinga
University of Twente
From Quality to Quantity

Quantitative system models

- Quantitative system models
- $z \leq 1 \quad z \geq 0.8$
- $y'' = -9.8 \quad y'' = 0$
- Open parachute
- Start dryer
- Heat = 0
- Heat = 5

Verification is usually boolean:
- either $A \models \Phi$ or $A \not\models \Phi$
- either $A \equiv_{\text{bis}} B$ or $A \not\equiv_{\text{bis}} B$

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

Problem:
- change values by 0.01
- $A \models \Phi$
- $A \equiv_{\text{bis}} B$
- $A' \not\models \Phi$
- $A' \not\equiv_{\text{bis}} B$

Fragility
Our opinion: verification should be \textit{quantitative}

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

\[
\begin{align*}
&\text{dist: 0} \quad \equiv \text{bis} \quad z \leq 0.5 \\
&\text{dist: 0.01} \quad \equiv_{\text{bis}} \quad z \leq 0.51
\end{align*}
\]
Quantitative system relations
- \(s \sqsubseteq t \iff \text{dist}(s,t)\)
  - how similar are two systems?
- linear dist: trace inclusion/equiv
- branching dist: (bi-)simulation

Quantitative logics
- \(s \models \phi \iff [\phi](s) \in [0,1]\)
  - how true is \(\phi\) in \(s\)?
- Quantitative LTL
- Quantitative CTL
The model

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

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

- Semantics: quantitative traces

  works as expected
Example: Kripke’s Washing Machine

\[ p = \text{power} \]
\[ h = \text{heating} \]
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*

\[ pd(\begin{array}{c} p=0.1 \\ q=0.8 \end{array}, \begin{array}{c} p=0.3 \\ q=0.7 \end{array}) = 0.2 \]

- How different are two traces? *Trace distance*

\[ ld^<(s,\sigma) = \sup_i pd^a(\sigma_i \rho_i) \]

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

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

*discounting*

... see next slide ....
Linear Distances

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

- Find same trace in \( B \) to match \( \sigma \)

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

- Find closest trace in \( B \) to match \( \sigma \)

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

- Trace at min dist

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

Find hardest trace in \( A \) to match \( \rho \)

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

- Trace at min dist

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

- Symmetric variant

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

- Find closest trace in \( B \) to match \( \rho \)
Ld<(A,B): example

dist: .2

dist: .1

dist: .2
Quantitative Linear Time Logic (QLTL)

(minimal) syntax

\[ \Phi ::= p \mid \Phi \lor \Phi \mid \neg \Phi \mid \Box \Phi \mid \Diamond \Phi \mid \Phi \oplus c \quad c \in [0,1] \]

semantics

\[ [p](\sigma) = \sigma_0(p) \]
\[ [\neg \Phi](\sigma) = 1 - [\Phi](\sigma) \]
\[ \Box \Phi(\sigma) = [\Phi](\sigma^1) \]
\[ \Phi_1 \lor \Phi_2(\sigma) = \max( [\Phi_1](\sigma), [\Phi_2](\sigma) ) \]
\[ \Diamond \Phi(\sigma) = \sup_i [\Phi](\sigma^i) \]
\[ \Phi \oplus c(\sigma) = \min([\Phi](\sigma) + c, 1) \]

\[ [\Phi](s) = \inf_{\sigma \in \text{tr}(s)} [\Phi](\sigma) \]
Semantics for \( \Diamond p \)

\( \sigma = \)

\[ \begin{align*}
\text{start} & \quad p=0 \quad h=0 \\
\text{warm} & \quad p=0.7 \quad h=0.6 \\
\text{rinse} & \quad p=0.4 \quad h=0 \\
\text{spin} & \quad p=0.6 \quad h=0.0 \\
\text{stop} & \quad p=0 \quad h=0 \\
\end{align*} \]

\( \lbrack \Diamond p \rbrack(\sigma) = \sup_i (\sigma^i)(p) = 0.7 \)

Washing Machine

\[ \lbrack \Diamond p \rbrack(s) = \inf_\sigma \lbrack \Diamond p \rbrack(\sigma) = 0.6 \]

\( \Diamond p = 0.6 \)

min peak consumption
Linear Characterization Results

**boolean:**

\[ A \equiv_{tr} B \iff \forall \phi \in \text{LTL}. \ A \models \phi \iff B \models \phi \]

\[ A \subseteq_{tr} B \iff \forall \phi \in \text{LTL}^+. \ A \models \phi \Rightarrow B \models \phi \]

**quantitative:**

\[ \text{ld}=(A, B) = \sup_{\phi \in \text{QLTL}} |[A](\phi) - [B](\phi)| \]

\[ \text{ld}< (A, B) = \sup_{\phi \in \text{QLTL}^+} |[A](\phi) - [B](\phi)| \]

Two directions:

- QLTL formulae cannot distinguish more than \( \text{ld} \) (\( \geq \)-direction)
- QLTL can distinguish arbitrary close to \( \text{ld} \) (\( \leq \)-direction)

(only \( \bigcirc \), \( \oplus \) needed in Q-logics)
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 \( R \)

- \( \sqsubseteq_{\text{sim}} \) 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. \( s \rightarrow s' \Rightarrow \exists t'. t \rightarrow t' \& d(s',t') \leq x \)
- \( \Rightarrow \) preserves \( d \)

- \( bd< \) is the smallest sim distance

\( s \sqsubseteq_{\text{sim}} t \) iff \( bd<(s,t) = 0 \)
bd< is the smallest distance such that for d(s,t) = x

1. d(s,t) ≥ pd(s,t)
2. s → s' ⇒ ∃ t'. t → t' & d(s',t') ≤ x

1. d(s,t) ≥ pd(s,t)
2. s → s' ⇒ \text{min}_{t'.t→t'} d(s',t') ≤ x

1. d(s,t) ≥ pd(s,t)
2. \text{max}_{s'.s→s'} \text{min}_{t'.t→t'} d(s',t') ≤ x

1. pd(s,t) ≤ d(s,t)
2. \text{max}_{s'.s→s'} \text{min}_{t'.t→t'} d(s',t') ≤ d(s,t)

pd(s,t) ∪ \text{max}_{s'.s→s'} \text{min}_{t'.t→t'} d(s',t') ≤ d(s,t)

bd< = \mu D . pd(s,t) ∪ \text{max}_{s'.s→s'} \text{min}_{t'.t→t'} D(s',t')

this gives fix point algorithm
Bisimulation Distance

simulation distance

\[ bd^< = \mu D \ . \ pd(s,t) \quad \sqcup \quad \max_{s' \cdot s \rightarrow s'} \min_{t' \cdot t \rightarrow t'} D(s',t') \]

bisimulation: symmetric version of simulation

\[ bd^\equiv = \mu D \ . \ pd(s,t) \quad \sqcup \quad \max_{s' \cdot s \rightarrow s'} \min_{t' \cdot t \rightarrow t'} D(s',t') \]
\[ \sqcup \quad \max_{t' \cdot t \rightarrow t'} \min_{s' \cdot s \rightarrow s'} D(s',t') \]
Quantitative Computation Tree Logic (QCTL)

(minimal) syntax

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

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

semantics

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

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

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

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

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

$$[\Box \Phi](\sigma) = [\Phi](\sigma^1)$$

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

In papers: Q\(\mu\) calculus
Branching Characterization Results

- **Boolean:**
  \[ A \equiv_{\text{bis}} B \iff \forall \phi \in \text{CTL}. \ A \models \phi \iff B \models \phi \]
  \[ A \preceq_{\text{sim}} B \iff \forall \phi \in \text{CTL}^+. \ A \models \phi \Rightarrow B \models \phi \]

- **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:**
  \[ A \equiv_{\text{bis}} B \quad \Rightarrow \quad A \equiv_{\text{tr}} B \]
  \[ \iff \quad B \text{ deterministic} \]

- **quantitative:**
  \[ \text{bd} = (A, B) \quad \geq \quad \text{ld} = (A, B) \quad \neq \quad B \text{ deterministic} \]

small branching distance \( \Rightarrow \) small linear distance
Quantitative logics QLTL, QCTL

- $s \models \phi \sim [\phi](s) \in [0,1]$ how true is $\phi$ in $s$?

Quantitative system relations

- Linear distances (trace inclusion/equivalence)
  - $s \equiv_{tr} t \sim \text{Id}(s,t)$ how similar are traces of $s,t$?
  - $s \subseteq_{tr} t \sim \text{Id}(s,t)$ how well can $t$ match traces $s$?
  - characterized by QLTL

- Branching distances (bisimulation/simulation)
  - $s \equiv_{bis} t \sim \text{Id}(s,t)$ how bisimilar are $s,t$?
  - $s \subseteq_{sim} t \sim \text{Id}(s,t)$ how well can steps of $t$ match steps of $s$?
  - characterized by QCTL
Rest of the talk

- **QTSs**
  1. linear setting
     - linear distance \( l_d \)
     - QLTL
  2. branching setting
     - branching distance \( b_d \)
     - QCTL

- **Stochastic Games**
  3. branching setting
     - a priori distance
     - a posteriori distance
     - \( Q\mu \)-calculus

- Conclusions
Stochastic Games

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

Properties

- coincide on MDPs, not in games
- a priori is canonical
  - 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
  - PI-1: a, b
  - PI-2: c, d
- Successor state is chosen probabilistically

Quantitative props = rewards

- Typical questions:
  - What is the (expected) reward player 1 is guaranteed to reach?
  - Which minimal reward can PI 1 maintain infinitely often?
  - Etc
Special cases

**Deterministic**

- **Single player**
  - LTSs
    - States: (r=0.1, q=0.3), (r=0.2, q=0.4), (r=0.9, q=0.3)
    - Transitions: a \rightarrow r=0.6, q=0.3, b \rightarrow r=0.1, q=0.3, e \rightarrow r=0.2, q=0.4

- **2 player**
  - Det Games
    - States: (r=0.1, q=0.3), (r=0.2, q=0.4), (r=0.9, q=0.3)
    - Transitions: a \rightarrow r=0.6, q=0.3, b \rightarrow r=0.1, q=0.3, c \rightarrow r=0.2, q=0.4

**Probabilistic**

- **Single player**
  - MDPs
    - States: (r=0.1, q=0.3), (r=0.6, q=0.3), (r=0.1, q=0.5), (r=0.2, q=0.4), (r=0.9, q=0.3)
    - Transitions: a \rightarrow 2/3, b \rightarrow 3/4, c \rightarrow 1/3

- **2 player**
  - Stoch Games
    - States: (r=0.1, q=0.3), (r=0.6, q=0.3), (r=0.1, q=0.5), (r=0.2, q=0.4), (r=0.9, q=0.3)
    - Transitions: a \rightarrow 2/3, b \rightarrow 3/4, c \rightarrow 1/3
MDPs: bisimulation distance

Similarity on MDPs

\[ (\mu, \nu) \in R \]

\[ \equiv \text{bis} \]

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

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

\[ \rightarrow \text{preserves } R \]

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

\[ d(\mu, \nu) \leq x \]

\[ \text{dist: } 0.1 \]

\[ 0.3 \]
\[ 0.5 \]
\[ 0.2 \]

\[ 0.5 \]
\[ 0.5 \]

\[ 0.3 \]
\[ 0.5 \]
\[ 0.2 \]

\[ 0.51 \]

\[ 0.49 \]

\[ \text{bd} = \mu D . \text{pd}(s, t) \cup \max_{s' \rightarrow \mu} \min_{t' \rightarrow \nu} D(\mu, \nu) \]
Distance between distributions

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

\[ d(\mu, \nu) = 0.2 \]

\[ E_{\mu}[k] = 0.5 \times 0.2 = 0.1 \]
\[ E_{\nu}[k] = 0.4 \times 0.2 = 0.08 \]
\[ E_{\mu}[k] - E_{\nu}[k] = 0.02 \]

- max difference in rewards
  \[ k(\ast) = 0 \quad k(\bullet) = 0.2 \]

- maximize over \( k \)
  \[ \max_k E_{\mu}[k] - E_{\nu}[k] \]

\[ \text{bd} = \mu \cdot D \cdot pd(s,t) \cup \]
\[ \max_{s' \rightarrow \mu} \min_{t' \rightarrow \nu} D(\mu, \nu) \]
\[ = \mu \cdot D \cdot pd(s,t) \cup \]
\[ \max_{s' \rightarrow \mu} \min_{t' \rightarrow \nu} E_{\mu}[k] - E_{\nu}[k] \]

A posteriori distance
**A posteriori distance**

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

**A priori distance**

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

best match \( t \rightarrow v \) depends on current goal \( k \)
MDPs: *a priori* and *a posteriori* coincide

\[ d_{\text{prio}} = \mu_D \cdot \text{pd}(s,t) \cup \max_k \max_s \rightarrow_{\mu} \min_t \rightarrow_{v} E\mu[k] - Ev[k] = \]

\[ = \mu_D \cdot \text{pd}(s,t) \cup \max_s \rightarrow_{\mu} \max_k \min_t \rightarrow_{v} E\mu[k] - Ev[k] = \]

\[ = \mu_D \cdot \text{pd}(s,t) \cup \max_s \rightarrow_{\mu} \min_t \rightarrow_{v} \max_k E\mu[k] - Ev[k] = \]

\[ d_{\text{post}} \]

by minimax
Games: a posteriori distance

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

- 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 $t$, 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 $t$, 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. $\text{prop}(s) = \text{prop}(t)$
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. $d(s,t) \leq ld(s,t)$
2. $\max x_1 \min y_1 \max y_2 \min x_2 \cdot d(\mu,\nu) =$

$= \max x_1 \min y_1 \max y_2 \min x_2 \cdot \max_k E_{x_1x_2}[k] - E_{y_1y_2}[k]$
Games: *a priori* vs *a posteriori* metrics

\[ d_{\text{post}} = \mu D \cdot \text{pd}(s,t) \sqcup \]

\[ \max x_1 \min y_1 \max y_2 \min x_2 \cdot \max_k E_{x_1x_2}[k] - E_{y_1y_2}[k] \]

\[ d_{\text{prio}} = \mu D \cdot \text{pd}(s,t) \sqcup \]

\[ \max_k \max x_1 \min y_1 \max y_2 \min x_2 \cdot E_{x_1x_2}[k] - E_{y_1y_2}[k] \]

Hence: \[ d_{\text{prio}} \leq d_{\text{post}} \]
Reciprocity of a priori metric

\[ \text{bd}_{	ext{prio}} = \mu \ D \ . \ \text{pd}(s,t) \]

\[ \max_k \ \max_{x_1} \min_{x_2} \max_{y_1} \min_{y_2} E_{x_1x_2}[k] - E_{y_1y_2}[k] \]

\[ = \mu \ D \ . \ \text{pd}(s,t) \]

\[ \max_k \ \max_{x_1} \min_{x_2} E_{x_1x_2}[k] - \max_{y_1} \min_{y_2} E_{y_1y_2}[k] \]

Determinacy of stoch games

\[ = \mu \ D \ . \ \text{pd}(s,t) \]

\[ \max_k \ \min_{x_2} \max_{x_1} E_{x_1x_2}[k] - \min_{y_2} \max_{y_1} E_{y_1y_2}[k] \]

Push though minus

\[ = \mu \ D \ . \ \text{pd}(s,t) \]

\[ \max_k \ \max_{y_2} \min_{y_1} E_{y_1y_2}[k] - \max_{x_1} \min_{x_2} E_{y_1y_2}[k] \]
Q\(\mu\) Quantitative \(\mu\)Calculus

- **syntax**

\[
\Phi ::= R \mid \Phi \lor \Phi \mid \neg \Phi \mid Z \mid \text{Pre}_i(\Phi) \mid \Phi \oplus c \mid \mu Z. \Phi
\]

- **semantics**

\[
\begin{align*}
[R](s) & = s(R) \\
[\neg \Phi](s) & = 1 - [\Phi](s) \\
[\Phi_1 \lor \Phi_2](s) & = \max( [\Phi_1](s), [\Phi_2](s) ) \\
[\Phi \oplus c](s) & = \max( [\Phi](s) + c, 1) \\
[\text{Pre}_i \Phi](\sigma) & = \text{maximal reward player } i \\
& \quad \text{can enforce in single step,} \\
& \quad \text{for rewards given by } \Phi
\end{align*}
\]
Branching Characterization Results

- *a priori* distance characterizes $Q_{\mu}$:

  $$bd_{\text{prio}}(A, B) = \sup_{\Phi \in Q_{\mu}^+} \[A\](\phi) - [B](\phi)$$

(similarly for symmetric variant)

- no characterization for $bd_{\text{prio}}$
Stochastic Games

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

Properties

- coincide on MDPs, not in games
- a priori is canonical
  - 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.**
  In *J. of Theoretical Computer Science'05*