Outline of the lectures

- Dec 13
- Dec 20
- Jan 10
- Jan 17
- Jan 24
Outline of the lectures

- The need for randomization
- Probabilistic automata
- Probabilistic bisimulation
- Probabilistic calculi
- Testing equivalence
- Introduction to probabilistic model checking and PRISM
- Metrics for probabilistic processes
- Verification of anonymity protocols: Dining Cryptographers, Crowds
Questions from the last lecture

Question 1:

- $P +_p Q \sqsubseteq_{\text{may}} \tau.P + \tau.Q$
- $\tau.P + \tau.Q \sqsubseteq_{\text{must}} P +_p Q$
Questions from the last lecture

**Question 2:** which of the following hold?

- $A\varphi \iff \mathcal{P}_{\geq \lambda} \varphi$?
- $A\varphi \Rightarrow \mathcal{P}_{\geq \lambda} \varphi$?
- $E\varphi \iff \mathcal{P}_{\geq \lambda} \varphi$?
- $E\varphi \Rightarrow \mathcal{P}_{\geq \lambda} \varphi$?
Questions from the last lecture

Question 3:

- $\Diamond \varphi \equiv \textbf{true} \cup \varphi$
- $\square \varphi \equiv \neg \Diamond \neg \varphi$
- $Pr^+_s \neg \psi = 1 - Pr^-_s \psi$
- $Pr^-_s \neg \psi = 1 - Pr^+_s \psi$

where the semantics of path formulas are extended with:
$s, s_1, \ldots \models \neg \psi$ iff $s, s_1, \ldots \not\models \psi$
Probabilistic bisimulation

A relation \( \mathcal{R} \subseteq S \times S \) is a \textit{strong probabilistic bisimulation} iff for all \( s_1, s_2 \in \mathcal{R} \) and for all \( a \in A \)

- if \( s_1 \xrightarrow{a} \mu_1 \) then \( \exists \mu_2 \) such that \( s_2 \xrightarrow{a} \mu_2 \) and \( \mu_1 \mathcal{R} \mu_2 \),
- if \( s_2 \xrightarrow{a} \mu_2 \) then \( \exists \mu_1 \) such that \( s_1 \xrightarrow{a} \mu_1 \) and \( \mu_1 \mathcal{R} \mu_2 \).

We write \( s_1 \sim s_2 \) if there is a strong bisimulation that relates them.
Probabilistic bisimulation

Transitions with different probabilities are allowed, as long as we go to equivalent states.

Diagram:

- States 1, 2, 3, 4, and 5 are connected by arrows labeled with 'a'.
- An arrow from state 1 to state 3 with a probability of 0.5 labeled as 'p'.

States 2 and 3 can reach states 4 and 5 respectively with the same label 'a'.
Probabilistic bisimulation

What about transitions to non-equivalent states?

We can argue that for $p$ close to 0.5, the processes are “close”. 
Pseudometrics

\[ m : S \times S \to [0, \infty) \text{ s.t.} \]

- \[ m(s, s) = 0 \]
- \[ m(s, t) = m(t, s) \]
- \[ m(s_1, s_3) \leq m(s_1, s_2) + m(s_2, s_3) \]

**Goal:** find a pseudometric \( m \) such that \( m(s, t) = 0 \iff s \sim t \)

Such a pseudometric is a metric on \( S/\sim \)
Metrics on probability distributions

- $m$: metric on $S$
- Goal: create metric $\hat{m}$ on $\text{Disc}(S)$
- $f : S \to \mathbb{R}$ is 1-Lipschitz wrt $m$ iff
  $$|f(s) - f(s')| \leq m(s, s') \quad \forall s, s' \in S$$
- $f(\mu) = \sum_s \mu(s)f(s)$
- Kantorovich metric:
  $$\hat{m}(\mu, \mu') = \sup \{|f(\mu) - f(\mu')| : f \text{ is 1-Lip wrt } m\}$$
Metrics on probability distributions

Kantorovich-Rubinstein theorem:

- Write $M(\mu, \mu')$ for the joint distributions $\alpha \in \text{Disc}(S \times S)$ with marginals $\mu, \mu'$, i.e.
  \[
  \alpha(s, S) = \mu(s) \quad \alpha(S, t) = \mu'(t)
  \]

- Then:
  \[
  \hat{m}(\mu, \mu') = \inf \left\{ \sum_{s,t} \alpha(s, t)m(s, t) \mid \alpha \in M(\mu, \mu') \right\}
  \]
Metrics on probability distributions

\( \hat{m}(\mu, \mu') \) can be computed as the solution to the following Linear program:

- **Variables:** \( \alpha_{s,t}, s, t \in S \)
- **minimize** \( \sum_{s,t} \alpha_{s,t} m(s, t) \)
- **subject to:**
  \[
  \sum_t \alpha_{s,t} = \mu(s) \quad \forall s \in S \\
  \sum_s \alpha_{s,t} = \mu'(t) \quad \forall t \in S \\
  \alpha_{s,t} \geq 0 \quad \forall s, t \in S
  \]
Complete Lattices

- Partially ordered set \((L, \leq)\)
  (reflexivity, antisymmetry, transitivity)

- All subsets of \(A \subseteq L\) have a supremum \(\bigvee A\) and an infimum \(\bigwedge A\)

- Examples:
  - \(2^S\) with \(\subseteq\)
  - \([0, 1]\) with \(\leq\)
  - Equivalence relations ordered by refinement

Question: what are the \(\bigvee, \bigwedge\) in each case?
Complete Lattices

- $\mathcal{M}$: the set of all 1-bounded pseudometrics on $S$
- Ordered by: $m \leq m'$ iff $m(s, t) \geq m'(s, t)$ for all $s, t \in S$
- $(\mathcal{M}, \leq)$ is a complete lattice
- What are $\top, \bot, \lor, \land$?
Knaster-Tarski theorem:

- 
  ▶ $(L, \leq)$ is a complete Lattice

- 
  ▶ $f$ is monotone: $a \leq b$ implies $f(a) \leq f(b)$

- 
  ▶ Then $f$ has a maximum and a minimum fixpoint (in fact the fixpoints form a complete Lattice under $\leq$)
The metric extension of bisimulation

General idea:
- Start from $m = \top$, i.e. everything is equivalent, which means distance 0 (similarly to the algorithm for computing bisimulation)
- The goal is that whenever $m(s, t) = a$ and $s \xrightarrow{a} \mu$, $t$ should match it with a transition $t \xrightarrow{b} \mu'$ such that $\hat{m}(\mu, \mu') \leq a$
- $F : \mathcal{M} \rightarrow \mathcal{M}$ updates $m$ so that the above property holds
- Our metric is the maximum fixpoint of $F$
Hausdorff distance

- Extend $m$ from $S$ to $2^S$

- $m(A, B) = \max\{\sup_{s \in A} \inf_{t \in B} m(s, t), \sup_{t \in B} \inf_{s \in A} m(s, t)\}$
The metric extension of bisimulation

- Define $F : \mathcal{M} \to \mathcal{M}$ as $F(m)(s, t) < \epsilon$ iff
  - $\forall s \xrightarrow{a} \mu \exists t \xrightarrow{a} \mu' : \hat{m}(\mu, \mu') < \epsilon$
  - $\forall t \xrightarrow{a} \mu \exists s \xrightarrow{a} \mu' : \hat{m}(\mu, \mu') < \epsilon$

- Define $s \xrightarrow{a} = \{ \mu | s \xrightarrow{a} \mu \}$

- Then
  $$F(m)(s, t) = \max_{a} \hat{m}(s \xrightarrow{a}, t \xrightarrow{a})$$
The metric extension of bisimulation

- $F$ is monotone, i.e. $m \leq m' \Rightarrow F(m) \leq F(m')$
- Hence, it has a maximum fixpoint
- We take $m$ as the maximum fixpoint of $F$
- It can be computed by iterating $F$ starting from $\top$
The metric extension of bisimulation

Lemma

$R$: equivalence relation on $S$, $m$: metric on $S$ s.t. $m(s, t) = 0 \iff sRt$. Then

$\hat{m}(\mu, \mu') \iff \mu R \mu'$

Theorem

$m \sim t$ iff $m(s, t) = 0$