Probabilistic Model Checking

Marta Kwiatkowska
Dave Parker

Oxford University Computing Laboratory

ESSLLI’10 Summer School, Copenhagen, August 2010
Course overview

• 5 lectures: Mon–Fri, 11am–12.30pm
  – Introduction
  – 1 – Discrete time Markov chains
  – 2 – Markov decision processes
  – 3 – Continuous–time Markov chains
  – 4 – Probabilistic model checking in practice
  – 5 – Probabilistic timed automata

• Course materials available here:
  – http://www.prismmodelchecker.org/lectures/esslli10/
  – lecture slides, reference list
<table>
<thead>
<tr>
<th>Time Type</th>
<th>Fully probabilistic</th>
<th>Nondeterministic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrete time</td>
<td>Discrete-time Markov chains (<em>DTMCs</em>)</td>
<td>Markov decision processes (<em>MDPs</em>) (probabilistic automata)</td>
</tr>
<tr>
<td>Continuous time</td>
<td>Continuous-time Markov chains (<em>CTMCs</em>)</td>
<td><em>CTMDPs/IMCs</em></td>
</tr>
</tbody>
</table>

*Probabilistic timed automata (*PTAs*)*
Part 3

Continuous-time Markov chains
Time in DTMCs

- Time in a DTMC (or MDP) proceeds in discrete steps

- Two possible interpretations:
  - accurate model of (discrete) time units
    - e.g. clock ticks in model of an embedded device
  - time-abstract
    - no information assumed about the time transitions take

- Continuous-time Markov chains (CTMCs)
  - dense model of time
  - transitions can occur at any (real-valued) time instant
  - modelled using exponential distributions
  - suits modelling of: performance/reliability (e.g. of computer networks, manufacturing systems, queueing networks), biological pathways, chemical reactions, ...
Overview (Part 3)

- Exponential distribution and its properties

- Continuous-time Markov chains (CTMCs)
  - definition, race conditions, examples
  - paths and probability spaces

- CSL: A temporal logic for CTMCs

- CSL model checking
  - uniformisation, steady-state probabilities

- Extensions: Costs & rewards
Continuous probability distributions

- **Defined by:**
  - cumulative distribution function
    \[
    F(t) = \Pr(X \leq t) = \int_{-\infty}^{t} f(x) \, dx
    \]
  - where \( f \) is the probability density function
  - \( \Pr(X=t) = 0 \) for all \( t \)

- **Example: uniform distribution: U(a,b)**
  \[
  f(t) = \begin{cases} 
    \frac{1}{b-a} & \text{if } a \leq t \leq b \\ 
    0 & \text{otherwise}
  \end{cases}
  \]
  \[
  F(t) = \begin{cases} 
    0 & \text{if } t < a \\ 
    \frac{t-a}{b-a} & \text{if } a \leq t < b \\ 
    1 & \text{if } t \geq b
  \end{cases}
  \]
Exponential distribution

• A continuous random variable $X$ is exponential with parameter $\lambda > 0$ if the density function is given by:

$$f(t) = \begin{cases} \lambda \cdot e^{-\lambda \cdot t} & \text{if } t > 0 \\ 0 & \text{otherwise} \end{cases}$$

$\lambda = \text{“rate”}$

• Cumulative distribution function (for $t \geq 0$):

$$F(t) = \Pr(X \leq t) = \int_0^t \lambda \cdot e^{-\lambda \cdot x} dx = [-e^{-\lambda \cdot x}]_0^t = 1 - e^{-\lambda \cdot t}$$

• Other properties:
  - negation: \( \Pr(X > t) = e^{-\lambda \cdot t} \)
  - mean (expectation): \( E[X] = \int_0^{\infty} x \cdot \lambda \cdot e^{-\lambda \cdot x} dx = \frac{1}{\lambda} \)
  - variance: \( \text{Var}(X) = \frac{1}{\lambda^2} \)
Exponential distribution – Examples

- The more $\lambda$ increases, the faster the c.d.f. approaches 1
Exponential distribution

- Adequate for modelling many real-life phenomena
  - failures
    - e.g. time before machine component fails
  - inter-arrival times
    - e.g. time before next call arrives to a call centre
  - biological systems
    - e.g. times for reactions between proteins to occur

- Maximal entropy if just the mean is known
  - i.e. best approximation when only mean is known

- Can approximate general distributions arbitrarily closely
  - phase-type distributions
Exponential distribution – Properties

• Two useful properties of the exponential distribution:
  
  • The exponential distribution is **memoryless**: 
    - \( \Pr( X > t_1 + t_2 \mid X > t_1 ) = \Pr( X > t_2 ) \)
    - it is the only memoryless continuous distribution
    - the discrete–time equivalent is the geometric distribution

• The **minimum** of two independent exponential distributions is an exponential distribution (parameter is sum)
  - \( X_1 \sim \text{Exponential}(\lambda_1), \ X_2 \sim \text{Exponential}(\lambda_2) \)
  - \( Y = \min(X_1,X_2) \sim \text{Exponential}(\lambda_1 + \lambda_2) \)
  - generalises to minimum of \( n \) distributions
Overview (Part 3)

- Exponential distribution and its properties

- **Continuous–time Markov chains (CTMCs)**
  - definition, race conditions, examples
  - paths and probability spaces

- CSL: A temporal logic for CTMCs

- CSL model checking
  - uniformisation, steady–state probabilities

- Extensions: Costs & rewards
Continuous-time Markov chains

- **Continuous-time Markov chains (CTMCs)**
  - labelled transition systems augmented with rates
  - continuous time delays, exponentially distributed

- **Formally, a CTMC C is a tuple (S,s_{init},R,L) where:**
  - S is a finite set of states (“state space”)
  - s_{init} ∈ S is the initial state
  - R : S × S → ℝ_{≥0} is the transition rate matrix
  - L : S → 2^{AP} is a labelling with atomic propositions

- **Transition rate matrix assigns rates to each pair of states**
  - used as a parameter to the exponential distribution
  - transition between s and s’ when R(s,s’)>0
  - probability triggered before t time units: 1 – e^{-R(s,s’)·t}
Simple CTMC example

- Modelling a queue of jobs
  - initially the queue is empty
  - jobs arrive with rate $3/2$ (i.e. mean inter-arrival time is $2/3$)
  - jobs are served with rate $3$ (i.e. mean service time is $1/3$)
  - maximum size of the queue is 3
  - state space: $S = \{s_i\}_{i=0..3}$ where $s_i$ indicates $i$ jobs in queue
Race conditions

• What happens when there exists multiple s’ with $R(s, s') > 0$?
  – **race condition**: first transition triggered determines next state
  – two questions:
    – 1. How long is spent in s before a transition occurs?
    – 2. Which transition is eventually taken?

• **1. Time spent in a state before a transition**
  – **minimum** of exponential distributions
  – exponential with parameter given by summation:
    \[ E(s) = \sum_{s' \in S} R(s, s') \]
  – probability of leaving a state s within $[0, t]$ is $1 - e^{-E(s) \cdot t}$
  – $E(s)$ is the **exit rate** of state s
  – s is called **absorbing** if $E(s) = 0$ (no outgoing transitions)
Race conditions...

2. Which transition is taken from state s?
   - the choice is independent of the time at which it occurs
   - e.g. if $X_1 \sim \text{Exponential}(\lambda_1)$, $X_2 \sim \text{Exponential}(\lambda_2)$
   - then the probability that $X_1 < X_2$ is $\frac{\lambda_1}{\lambda_1 + \lambda_2}$
   - more generally, the probability is given by...

- The embedded DTMC: $\text{emb}(C) = (S, s_{\text{init}}, P^{\text{emb}(C)}, L)$
  - state space, initial state and labelling as the CTMC
  - for any $s, s' \in S$
    \[
    P^{\text{emb}(C)}(s, s') = \begin{cases} 
      \frac{R(s, s')}{E(s)} & \text{if } E(s) > 0 \\
      1 & \text{if } E(s) = 0 \text{ and } s = s' \\
      0 & \text{otherwise}
    \end{cases}
    \]

- Probability that next state from s is s' given by $P^{\text{emb}(C)}(s, s')$
Two interpretations of a CTMC

• Consider a (non-absorbing) state $s \in S$ with multiple outgoing transitions, i.e. multiple $s' \in S$ with $R(s,s') > 0$

• **1. Race condition**
  – each transition triggered after exponentially distributed delay
    • probability triggered before $t$ time units: $1 - e^{-R(s,s') \cdot t}$
  – first transition triggered determines the next state

• **2. Separate delay/transition**
  – remain in $s$ for delay exponentially distributed with rate $E(s)$
    • i.e. probability of taking an outgoing transition from $s$ within $[0,t]$ is given by $1 - e^{-E(s) \cdot t}$
  – probability that next state is $s'$ is given by $P_{\text{emb}(C)}(s,s')$
    • i.e. $R(s,s')/E(s) = R(s,s') / \Sigma_{s' \in S} R(s,s')$
Continuous-time Markov chains

- **Infinitesimal generator matrix**

\[
Q(s, s') = \left\{ \begin{array}{ll}
R(s, s') & s \neq s' \\
- \sum_{s \neq s'} R(s, s') & \text{otherwise}
\end{array} \right.
\]

- **Alternative definition: a CTMC is:**
  - a family of random variables \( \{ X(t) \mid t \in \mathbb{R}_{\geq 0} \} \)
  - \( X(t) \) are observations made at time instant \( t \)
  - i.e. \( X(t) \) is the state of the system at time instant \( t \)
  - which satisfies...

- **Memoryless (Markov property)**

\[
P[X(t_k) = s_k \mid X(t_{k-1}) = s_{k-1}, \ldots, X(t_0) = s_0] = P[X(t_k) = s_k \mid X(t_{k-1}) = s_{k-1}]
\]
Simple CTMC example...

$C = (S, s_{\text{init}}, R, L)$

$S = \{s_0, s_1, s_2, s_3\}$

$s_{\text{init}} = s_0$

$AP = \{\text{empty}, \text{full}\}$

$L(s_0) = \{\text{empty}\}, L(s_1) = L(s_2) = \emptyset$ and $L(s_3) = \{\text{full}\}$

\[
R = \begin{bmatrix}
0 & 3/2 & 0 & 0 \\
3 & 0 & 3/2 & 0 \\
0 & 3 & 0 & 3/2 \\
0 & 0 & 3 & 0
\end{bmatrix}
\]

$P^{\text{emb}(C)} = \begin{bmatrix}
0 & 1 & 0 & 0 \\
2/3 & 0 & 1/3 & 0 \\
0 & 2/3 & 0 & 1/3 \\
0 & 0 & 1 & 0
\end{bmatrix}$

$Q = \begin{bmatrix}
-3/2 & 3/2 & 0 & 0 \\
3 & -9/2 & 3/2 & 0 \\
0 & 3 & -9/2 & 3/2 \\
0 & 0 & 3 & -3
\end{bmatrix}$

- transition rate matrix
- embedded DTMC
- infinitesimal generator matrix
Example 2

- 3 machines, each can fail independently
  - failure rate $\lambda$, i.e. mean-time to failure (MTTF) = $1 / \lambda$
  - modelled as exponential distributions
- One repair unit
  - repairs a single machine at rate $\mu$ (also exponential)
- State space:
  - $S = \{s_i\}_{i=0..3}$ where $s_i$ indicates $i$ machines operational
Example 3

• Chemical reaction system: two species A and B

• Two reactions:

\[
\begin{align*}
\text{A} + \text{B} & \xrightleftharpoons[k_2]{k_1} \text{AB} \\
\text{A} & \xrightarrow{k_3} \\
\end{align*}
\]

– reversible reaction under which species A and B bind to form AB (forwards rate = \(|A| \cdot |B| \cdot k_1\), backwards rate = \(|AB| \cdot k_2\))
– degradation of A (rate \(|A| \cdot k_3\))
– \(|X|\) denotes number of molecules of species \(X\)

• CTMC with state space

– \((|A|, |B|, |AB|)\)
– initially (2,2,0)
Paths of a CTMC

- **An infinite path** $\omega$ is a sequence $s_0 t_0 s_1 t_1 s_2 t_2 \ldots$ such that
  - $R(s_i, s_{i+1}) > 0$ and $t_i \in \mathbb{R}_{>0}$ for all $i \in \mathbb{N}$
  - amount of time spent in the $j$th state: $\text{time}(\omega, j) = t_j$
  - state occupied at time $t$: $\omega @ t = s_j$
    where $j$ smallest index such that $\sum_{i \leq j} t_j \geq t$

- **A finite path** is a sequence $s_0 t_0 s_1 t_1 s_2 t_2 \ldots t_{k-1} s_k$ such that
  - $R(s_i, s_{i+1}) > 0$ and $t_i \in \mathbb{R}_{>0}$ for all $i < k$
  - $s_k$ is absorbing ($R(s, s') = 0$ for all $s' \in S$)
  - amount of time spent in the $i$th state only defined for $j \leq k$:
    - $\text{time}(\omega, j) = t_j$ if $j < k$ and $\text{time}(\omega, j) = \infty$ if $j = k$
  - state occupied at time $t$: if $t \leq \sum_{i \leq k} t_j$ then $\omega @ t$ as above
    otherwise $t > \sum_{i \leq k} t_j$ then $\omega @ t = s_k$

- **Path(s)** denotes all infinite and finite paths starting in $s$
Recall: Probability spaces

- A σ-algebra (or σ-field) on Ω is a family Σ of subsets of Ω closed under complementation and countable union, i.e.:
  - if $A \in \Sigma$, the complement $\Omega \setminus A$ is in $\Sigma$
  - if $A_i \in \Sigma$ for $i \in \mathbb{N}$, the union $\bigcup_i A_i$ is in $\Sigma$
  - the empty set $\emptyset$ is in $\Sigma$
- Elements of $\Sigma$ are called measurable sets or events
- Theorem: For any family $F$ of subsets of $\Omega$, there exists a unique smallest σ-algebra on $\Omega$ containing $F$
- Probability space $(\Omega, \Sigma, \Pr)$
  - $\Omega$ is the sample space
  - $\Sigma$ is the set of events: σ-algebra on $\Omega$
  - $\Pr : \Sigma \rightarrow [0,1]$ is the probability measure:
    $\Pr(\Omega) = 1$ and $\Pr(\bigcup_i A_i) = \sum_i \Pr(A_i)$ for countable disjoint $A_i$
Probability space

• **Sample space:** Path(s) (set of all paths from a state s)

• **Events:** sets of infinite paths

• **Basic events:** cylinders
  - cylinders = sets of paths with common finite prefix
  - include **time intervals** in cylinders

• **Cylinder** is a sequence $s_0,l_0,s_1,l_1,...,l_{n-1},s_n$
  - $s_0,s_1,s_2,...,s_n$ sequence of states where $R(s_i,s_{i+1}) > 0$ for $i < n$
  - $l_0,l_1,l_2,...,l_{n-1}$ sequence of nonempty intervals of $\mathbb{R}_{\geq 0}$

• **Cyl(s_0,l_0,s_1,l_1,...,l_{n-1},s_n)** set of (infinite and finite paths):
  - $\omega(i)=s_i$ for all $i \leq n$ and $\text{time}(\omega,i) \in l_i$ for all $i < n$
Probability space

- Define measure over cylinders by induction

- $\Pr_s(Cyl(s)) = 1$

- $\Pr_s(Cyl(s, l, s_1, l_1, \ldots, l_{n-1}, s_n, l', s'))$ equals:
  
  $\Pr_s(Cyl(s, l, s_1, l_1, \ldots, l_{n-1}, s_n)) \cdot P_{emb(C)}^{s_n}(s_n, s') \cdot \left(e^{-E(s_n) \cdot \text{inf} l'} - e^{-E(s_n) \cdot \text{sup} l'}\right)$

- Probability transition from $s_n$ to $s'$ (defined using embedded DTMC)

- Probability time spent in state $s_n$ is within the interval $l'$
Probability space

- **Probability space** \((\text{Path}(s), \Sigma_{\text{Path}(s)}, \text{Pr}_s)\) \[\text{BHHK03}\]

- **Sample space** \(\Omega = \text{Path}(s)\) (infinite and finite paths)

- **Event set** \(\Sigma_{\text{Path}(s)}\)
  - least \(\sigma\)-algebra on \(\text{Path}(s)\) containing all cylinders sets \(\text{Cyl}(s_0, I_0, \ldots, I_{n-1}, s_n)\) where:
    - \(s_0, \ldots, s_n\) ranges over all state sequences with \(R(s_i, s_{i+1}) > 0\) for all \(i\)
    - \(I_0, \ldots, I_{n-1}\) ranges over all sequences of non-empty intervals in \(\mathbb{R}_{\geq 0}\)
      (where intervals are bounded by rationals)

- **Probability measure** \(\text{Pr}_s\)
  - \(\text{Pr}_s\) extends uniquely from probability defined over cylinders
Probability space – Example

• Probability of leaving the initial state $s_0$ and moving to state $s_1$ within the first 2 time units of operation?

• Cylinder $\text{Cyl}(s_0,(0,2],s_1)$

• $\Pr_{s_0}(\text{Cyl}(s_0,(0,2],s_1))$

\[
= \Pr_{s_0}(\text{Cyl}(s_0)) \cdot P_{\text{emb}(C)}(s_0,s_1) \cdot (e^{-E(s_0) \cdot 0} - e^{-E(s_0) \cdot 2})
= 1 \cdot 1 \cdot (e^{-3/2 \cdot 0} - e^{-3/2 \cdot 2})
= 1 - e^{-3}
\approx 0.95021
\]
Transient and steady-state behaviour

- **Transient behaviour**
  - state of the model at a particular *time instant*
  - $\pi_{s,t}^C(s')$ is probability of, having started in state $s$, being in state $s'$ at time $t$ (in CTMC $C$)
  - $\pi_{s,t}^C(s') = \Pr_s\{\omega \in \text{Path}^C(s) | \omega @t = s' \}$

- **Steady-state behaviour**
  - state of the model in the *long-run*
  - $\pi_s^C(s')$ is probability of, having started in state $s$, being in state $s'$ in the long run
  - $\pi_s^C(s') = \lim_{t \to \infty} \pi_{s,t}^C(s')$
  - intuitively: long-run percentage of time spent in each state
Overview (Part 3)

• Exponential distribution and its properties

• Continuous–time Markov chains (CTMCs)
  – definition, race conditions, examples
  – paths and probability spaces

• CSL: A temporal logic for CTMCs

• CSL model checking
  – uniformisation, steady–state probabilities

• Extensions: Costs & rewards
CSL

- Temporal logic for describing properties of CTMCs
  - CSL = Continuous Stochastic Logic [ASSB00,BHHK03]
  - extension of (non–probabilistic) temporal logic CTL
  - transient, steady–state and path–based properties

- Key additions:
  - probabilistic operator $P$ (like PCTL)
  - steady state operator $S$

- Example: $\text{down} \rightarrow P_{>0.75} [ \neg \text{fail} U_{[1,2.5]} \text{ up } ]$
  - when a shutdown occurs, the probability of a system recovery being completed between 1 and 2.5 hours without further failure is greater than 0.75

- Example: $S_{<0.1} [ \text{insufficient_routers} ]$
  - in the long run, the chance that an inadequate number of routers are operational is less than 0.1
CSL syntax

- **CSL syntax:**

  \[ \phi ::= \text{true} \mid a \mid \phi \land \phi \mid \neg \phi \mid P_{\sim p} [\psi] \mid S_{\sim p} [\phi] \quad \text{(state formulae)} \]

  \[ \psi ::= X \phi \mid \phi \ U \ I \ \phi \quad \text{(path formulae)} \]

- where \( a \) is an atomic proposition, \( I \) interval of \( \mathbb{R}_{\geq 0} \), \( p \in [0,1] \), and \( \sim \in \{<,>,\leq,\geq\} \)

- unbounded until \( U \) is a special case: \( \phi_1 U \phi_2 \equiv \phi_1 U^{[0,\infty)} \phi_2 \)

- **Quantitative properties:** \( P_{\sim \approx} [\psi] \) and \( S_{\sim \approx} [\phi] \)

  - where \( P/S \) is the outermost operator
CSL semantics for CTMCs

- CSL formulae interpreted over states of a CTMC
  - $s \vDash \phi$ denotes $\phi$ is “true in state $s$” or “satisfied in state $s$”

- Semantics of state formulae:
  - for a state $s$ of the CTMC $(S, s_{\text{init}}, R, L)$:
    - $s \vDash a \iff a \in L(s)$
    - $s \vDash \phi_1 \land \phi_2 \iff s \vDash \phi_1$ and $s \vDash \phi_2$
    - $s \vDash \neg \phi \iff s \vDash \phi$ is false
    - $s \vDash P_{\sim p} [\psi] \iff \text{Prob}(s, \psi) \sim p$
    - $s \vDash S_{\sim p} [\phi] \iff \sum_{s'} s' \vDash_{s} \pi_{s}(s') \sim p$

Probability of, starting in state $s$, being in state $s'$ in the long run

Probability of, starting in state $s$, satisfying the path formula $\psi$
CSL semantics for CTMCs

- **Prob(s, ψ)** is the probability, starting in state s, of satisfying the path formula ψ
  - \( \text{Prob}(s, \psi) = \Pr_s \{ \omega \in \text{Path}_s \mid \omega \models \psi \} \)

- **Semantics of path formulae:**
  - for a path \( \omega \) of the CTMC:
    - \( \omega \models X \phi \iff \omega(1) \) is defined and \( \omega(1) \models \phi \)
    - \( \omega \models \phi_1 \cup^I \phi_2 \iff \exists t \in I. (\omega@t \models \phi_2 \land \forall t'<t. \omega@t' \models \phi_1) \)

  - if \( \omega(0) \) is absorbing, \( \omega(1) \) not defined

  there exists a time instant in the interval I where \( \phi_2 \) is true and \( \phi_1 \) is true at all preceding time instants
**Case study: Cluster of workstations [HHK00]**

- two sub-clusters (N workstations in each cluster)
- star topology with a central switch
- components can break down, single repair unit

- **minimum QoS**: at least $\frac{3}{4}$ of the workstations operational and connected via switches
- **premium QoS**: all workstations operational and connected via switches
CSL example – Workstation cluster

- $S = ? [\text{ minimum }]$
  - the probability in the long run of having minimum QoS

- $P = ? [F_{[t,t]} \text{ minimum }]$
  - the (transient) probability at time instant $t$ of minimum QoS

- $P < 0.05 [F_{[0,10]} \neg \text{minimum}]$
  - the probability that the QoS drops below minimum within 10 hours is less than 0.05

- $\neg \text{minimum} \rightarrow P < 0.1 [F_{[0,2]} \neg \text{minimum}]$
  - when facing insufficient QoS, the chance of facing the same problem after 2 hours is less than 0.1
• **minimum → P >0.8 [ minimum U^{[0,t]} premium ]**
  
  – the probability of going from minimum to premium QoS within t hours without violating minimum QoS is at least 0.8

• **P =? [ ¬minimum U^{[t,∞)} minimum ]**
  
  – the chance it takes more than t time units to recover from insufficient QoS

• **¬r_switch_up → P <0.1 [ ¬r_switch_up U ¬l_switch_up ]**
  
  – if the right switch has failed, the probability of the left switch failing before it is repaired is less than 0.1

• **P =? [ F^{[2,∞)} S >0.9[ minimum ] ]**
  
  – the probability of it taking more than 2 hours to get to a state from which the long-run probability of minimum QoS is >0.9
Overview (Part 3)

- Exponential distribution and its properties

- Continuous-time Markov chains (CTMCs)
  - definition, race conditions, examples
  - paths and probability spaces

- CSL: A temporal logic for CTMCs

- **CSL model checking**
  - uniformisation, steady-state probabilities

- Extensions: Costs & rewards
CSL model checking

- Model checking a CSL formula $\phi$ on a CTMC
  - basic algorithm proceeds by induction on parse tree of $\phi$
  - non-probabilistic operators (true, $a$, $\neg$, $\land$) identical to PCTL

- Main task: computing probabilities for $P_{\neg_p}[\cdot]$ and $S_{\neg_p}[\cdot]$  

- Untimed properties can be verified on the embedded DTMC
  - properties of the form: $P_{\neg_p}[X\phi]$ or $P_{\neg_p}[\phi_1 U \phi_2]$
  - use algorithms for checking PCTL against DTMCs

- Which leaves...
  - time-bounded until operator: $P_{\neg_p}[\phi U^I \phi]$
  - steady-state operator: $S_{\neg_p}[\phi]$
Model checking – Time–bounded until

• Compute $\text{Prob}(s, \phi_1 U^I \phi_2)$ for all states where $I$ is an arbitrary interval of the non-negative real numbers

• Note:
  – $\text{Prob}(s, \phi_1 U^I \phi_2) = \text{Prob}(s, \phi_1 U^{\text{cl}(I)} \phi_2)$
    where $\text{cl}(I)$ denotes the closure of the interval $I$
  – $\text{Prob}(s, \phi_1 U^{[0,\infty)} \phi_2) = \text{Prob}^{\text{emb}(C)}(s, \phi_1 U \phi_2)$
    where $\text{emb}(C)$ is the embedded DTMC

• Therefore, 3 remaining cases to consider:
  – $I = [0,t]$ for some $t \in \mathbb{R}_{\geq 0}$ (described in this lecture)
  – $I = [t,t']$ for some $t \leq t' \in \mathbb{R}_{\geq 0}$ or $I = [t,\infty)$ for some $t \in \mathbb{R}_{\geq 0}$

• Two methods: 1. Integral equations; 2. Uniformisation
Time-bounded until (integral equations)

- Computing the probabilities reduces to determining the least solution of the following set of integral equations:

- \( \text{Prob}(s, \phi_1 U^{[0,t]} \phi_2) \) equals
  - 1 if \( s \in \text{Sat}(\phi_2) \),
  - 0 if \( s \in \text{Sat}(\neg \phi_1 \land \neg \phi_2) \)
  - and otherwise equals

\[
\int_0^t \sum_{s' \in S} \left( P_{\text{emb}(C)}(s,s') \cdot E(s) \cdot e^{-E(s) \cdot x} \right) \cdot \text{Prob}(s',\phi_1 U^{[0,t-x]} \phi_2) \, dx
\]

- One possibility: solve these integrals numerically
  - e.g. trapezoidal, Simpson and Romberg integration
  - expensive, possible problems with numerical stability
Time-bounded until (uniformisation)

• **Reduction to transient analysis…**
  – on a modified CTMC $C'$

• **Make all $\phi_2$ states absorbing**
  – in such a state $\phi_1 \cup [0,x] \phi_2$
    holds with **probability 1**

• **Make all $\neg \phi_1 \land \neg \phi_2$ states absorbing**
  – in such a state $\phi_1 \cup [0,x] \phi_2$
    holds with **probability 0**

• **Formally:** modified CTMC $C' = C[\phi_2][\neg \phi_1 \land \neg \phi_2]$
  – where for CTMC $C=(S,s_{init},R,L)$, let $C[\theta]=(S,s_{init},R[\theta],L)$ where
    $R[\theta](s,s')=R(s,s')$ if $s \notin \text{Sat}(\theta)$ and 0 otherwise
• Problem then reduces to calculating **transient probabilities** in the modified CTMC $C'$:

$$\text{Prob}(s, \phi_1 \cup^{[0,t]} \phi_2) = \sum_{s' \in \text{Sat}(\phi_2)} \pi_{s,t}^{C'}(s')$$

- where $\phi_2$ is a 0–1 vector characterising $\phi_2$

- and $\Pi_t^{C'}$ is the matrix of all transient probabilities in $C'$

• To compute for all states $s$:

$$\text{Prob}(\phi_1 \cup^{[0,t]} \phi_2) = \Pi_t^{C'} \cdot \phi_2$$
Computing transient probabilities

- $\Pi_t$ – matrix of transient probabilities
  - $\Pi_t(s,s') = \pi_{s,t}(s')$

- $\Pi_t$ solution of the differential equation: $\Pi_t' = \Pi_t \cdot Q$
  - $Q$ infinitesimal generator matrix

- Can be expressed as a matrix exponential and therefore evaluated as a power series:
  $$\Pi_t = e^{Q \cdot t} = \sum_{i=0}^{\infty} \frac{(Q \cdot t)^i}{i!}$$
  - computation potentially unstable
  - probabilities instead computed using uniformisation
Uniformisation

- Uniformised DTMC $\text{unif}(C)$ of CTMC $C = (S, s_{\text{init}}, R, L)$:
  - $\text{unif}(C) = (S, s_{\text{init}}, P^{\text{unif}(C)}, L)$
  - set of states, initial state and labelling the same as $C$
  - $P^{\text{unif}(C)} = I + Q/q$
  - $I$ is the $|S| \times |S|$ identity matrix
  - $q \geq \max \{ E(s) \mid s \in S \}$ is the uniformisation rate

- Each time step (epoch) of uniformised DTMC corresponds to one exponentially distributed delay with rate $q$
  - if $E(s) = q$ transitions the same as embedded DTMC (residence time has the same distribution as one epoch)
  - if $E(s) < q$ add self loop with probability $1 - E(s)/q$ (residence time longer than $1/q$ so one epoch may not be ‘long enough’)
Uniformisation – Example

- **CTMC C:**
  
  \[\begin{array}{cccc}
  s_0 & s_1 & s_2 & s_3 \\
  {\text{empty}} & 3/2 & 3/2 & 3/2 \\
  3 & 3 & 3 & \{\text{full}\}
  \end{array}\]

- **Uniformised DTMC unif(C)**
  - let uniformisation rate \( q = \max_s \{ E(s) \} = 4.5 \)
  
  \[\begin{align*}
  P_{\text{unif(C)}} &= I + Q/q \\
  R &= \begin{bmatrix}
  0 & 3/2 & 0 & 0 \\
  3 & 0 & 3/2 & 0 \\
  0 & 3 & 0 & 3/2 \\
  0 & 0 & 3 & 0
  \end{bmatrix}
  \]

  \[\begin{align*}
  P_{\text{unif}(C)} &= \begin{bmatrix}
  2/3 & 1/3 & 0 & 0 \\
  2/3 & 0 & 1/3 & 0 \\
  0 & 2/3 & 0 & 1/3 \\
  0 & 0 & 2/3 & 1/3
  \end{bmatrix}
  \]
Uniformisation

- Using the uniformised DTMC the transient probabilities can be expressed by:

\[ \Pi_t = e^{Q \cdot t} = e^{q \cdot (P^\text{unif}(C) - I) \cdot t} = e^{(q \cdot t) \cdot P^\text{unif}(C)} \cdot e^{-q \cdot t} \]

\[ = e^{-q \cdot t} \cdot \left( \sum_{i=0}^{\infty} \frac{(q \cdot t)^i}{i!} \cdot \left( P^\text{unif}(C) \right)^i \right) \]

\[ = \sum_{i=0}^{\infty} \left( e^{-q \cdot t} \cdot \frac{(q \cdot t)^i}{i!} \right) \left( P^\text{unif}(C) \right)^i \]

\[ = \sum_{i=0}^{\infty} \gamma_{q \cdot t, i} \cdot \left( P^\text{unif}(C) \right)^i \]

\[ P^\text{unif}(C) \text{ stochastic (all entries in [0,1] & rows sum to 1), therefore computations with } P \text{ more numerically stable than } Q \]

ith Poisson probability with parameter \( q \cdot t \)
Uniformisation

\[ \Pi_t = \sum_{i=0}^{\infty} \gamma_{q \cdot t, i} \cdot (P_{\text{unif}(C)})^i \]

- \((P_{\text{unif}(C)})^i\) is probability of jumping between each pair of states in \(i\) steps

- \(\gamma_{q \cdot t, i}\) is the \(i\)th Poisson probability with parameter \(q \cdot t\)
  - the probability of \(i\) steps occurring in time \(t\), given each has delay exponentially distributed with rate \(q\)

- Can truncate the (infinite) summation using the techniques of Fox and Glynn [FG88], which allow efficient computation of the Poisson probabilities
Recall that for model checking, we require:

\[
\text{Prob}(\phi_1 U^{[0,t]} \phi_2) = \prod_t \cdot \phi_2
\]

So, using uniformisation:

\[
\text{Prob}(\phi_1 U^{[0,t]} \phi_2) = \sum_{i=0}^{\infty} \gamma_{q\cdot t, i} \cdot \left( P_{\text{unif}(C')}^i \right) \cdot \phi_2
\]

This can be computed efficiently using matrix–vector multiplication (avoiding matrix powers):

\[
\left( P_{\text{unif}(C')}^0 \right) \cdot \phi_2 = \phi_2
\]
\[
\left( P_{\text{unif}(C')}^{i+1} \right) \cdot \phi_2 = P_{\text{unif}(C')} \cdot \left( \left( P_{\text{unif}(C')}^i \right) \cdot \phi_2 \right)
\]
Time-bounded until – Example

• $P_{>0.65} [ F^{[0,7.5]} \text{ full } ] \equiv P_{>0.65} [ \text{ true } U^{[0,7.5]} \text{ full } ]$
  – “probability of the queue becoming full within 7.5 time units”

• State $s_3$ satisfies full and no states satisfy $\neg \text{true}$
  – in $C[\text{full}][\neg \text{true} \land \neg \text{full}]$ only state $s_3$ made absorbing

\[
\begin{bmatrix}
2/3 & 1/3 & 0 & 0 \\
2/3 & 0 & 1/3 & 0 \\
0 & 2/3 & 0 & 1/3 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]

matrix of $\text{unif}(C[\text{full}][\neg \text{true} \land \neg \text{full}])$
with uniformisation rate $\max_{s \in S} E(s) = 4.5$

$s_3$ made absorbing
Time-bounded until – Example

- Computing the summation of matrix-vector multiplications

\[
\text{Prob}(\phi_1 \cup_{[0,t]} \phi_2) = \sum_{i=0}^{\infty} \left( \gamma_{q \cdot t, i} \cdot \left( P^{\text{unif}(C')} \right)^i \cdot \phi_2 \right)
\]

- yields \( \text{Prob}( F^{[0,7.5]} \text{ full } ) \approx [ 0.6482, 0.6823, 0.7811, 1 ] \)

- \( P_{>0.65}[ F^{[0,7.5]} \text{ full } ] \) satisfied in states \( s_1, s_2 \) and \( s_3 \)
A state $s$ satisfies the formula $S \sim_p \phi$ if $\sum_{s'} = \phi \pi^C_s(s') \sim p$

- $\pi^C_s(s')$ is the probability, having started in state $s$, of being in state $s'$ in the long run
- thus model checking reduces to computing and then summing steady-state probabilities for the CTMC

Steady-state probabilities: $\pi^C_s(s') = \lim_{t \to \infty} \pi^C_{s,t}(s')$

- limit exists for all finite CTMCs
- need to consider underlying graph structure of CTMC
- i.e. its bottom strongly connected components (BSCCs)
- irreducible CTMC (comprises one BSCC)
  - solution of one linear equation system
- reducible CTMC (multiple BSCCs)
  - solve for each BSCC, combine results
Irreducible CTMCs

• For an irreducible CTMC:
  – the steady-state probabilities are independent of the starting state: denote the steady state probabilities by $\pi^C(s')$

• These probabilities can be computed as
  – the unique solution of the linear equation system:
    
    $$\pi^C \cdot Q = \mathbf{0} \quad \text{and} \quad \sum_{s \in S} \pi^C(s) = 1$$

    where $Q$ is the infinitesimal generator matrix of $C$

• Solved by standard means:
  – direct methods, such as Gaussian elimination
  – iterative methods, such as Jacobi and Gauss–Seidel
Balance equations

For all \( s \in S \):

\[
\pi^C(s) \cdot (\sum_{s' \neq s} R(s,s')) + \sum_{s' \neq s} \pi^C(s') \cdot R(s',s) = 0
\]

\[\Leftrightarrow\]

\[
\pi^C(s) \cdot \sum_{s' \neq s} R(s,s') = \sum_{s' \neq s} \pi^C(s') \cdot R(s',s)
\]

Equivalent to: \( \pi^C \cdot P = \pi^C \) where \( P \) is matrix for embedded DTMC

balance the rate of leaving and entering a state

normalisation
• Model check $S_{<0.1}$ [ full ] on CTMC:

- CTMC is irreducible (comprises a single BSCC)
  - steady state probabilities independent of starting state

• Solve: $\pi \cdot Q = 0$ and $\sum \pi(s) = 1$
Steady-state – Example

- **Model check** $S_{<0.1}[$ full $]$ on CTMC:

- **Solve:**

  - $-3/2 \cdot \pi(s_0) + 3 \cdot \pi(s_1) = 0$
  - $3/2 \cdot \pi(s_0) - 9/2 \cdot \pi(s_1) + 3 \cdot \pi(s_2) = 0$
  - $3/2 \cdot \pi(s_1) - 9/2 \cdot \pi(s_2) + 3 \cdot \pi(s_3) = 0$
  - $3/2 \cdot \pi(s_2) - 3 \cdot \pi(s_3) = 0$

  - solution: $\pi = [8/15, 4/15, 2/15, 1/15]$

- $\Sigma_{s' \models \text{Sat(full)}} \pi(s') = 1/15 < 0.1$

- so all states satisfy $S_{<0.1}[$ full $]$
Reducible CTMCs

- For a reducible CTMC:
  - the steady-state probabilities $\pi^C(s')$ depend on start state $s$

- Find all BSCCs of CTMC, denoted bscc(C)

- Compute:
  - steady-state probabilities $\pi^T$ of sub-CTMC for each BSCC $T$
  - probability $\text{Prob}^{\text{emb}(C)}(s, F T)$ of reaching each $T$ from $s$

- Then:
  $$\pi^C_s(s') = \begin{cases} 
\text{Prob}^{\text{emb}(C)}(s, F T) \cdot \pi^T(s') & \text{if } s' \in T \text{ for some } T \in \text{bscc}(C) \\
0 & \text{otherwise}
\end{cases}$$
CSL model checking complexity

• For CSL model checking of a CTMC, complexity is:
  – linear in $|\Phi|$ and polynomial in $|S|$
  – linear in $q \cdot t_{\text{max}}$ ($t_{\text{max}}$ is maximum finite bound in intervals)

• Unbounded until $(P_{\sim p}[\Phi_1 \cup [0,\infty) \Phi_2])$ and steady-state $(S_{\sim p}[\Phi])$
  – require solution of linear equation system of size $|S|$
  – can be solved with Gaussian elimination: cubic in $|S|$
  – precomputation algorithms (max $|S|$ steps)

• Time–bounded until $(P_{\sim p}[\Phi_1 \cup I \Phi_2])$
  – at most two iterative sequences of matrix–vector products
  – operation is quadratic in the size of the matrix, i.e. $|S|$
  – total number of iterations bounded by Fox and Glynn
  – the bound is linear in the size of $q \cdot t$ (q uniformisation rate)
Overview (Part 3)

• Exponential distribution and its properties

• Continuous-time Markov chains (CTMCs)
  – definition, race conditions, examples
  – paths and probability spaces

• CSL: A temporal logic for CTMCs

• CSL model checking
  – uniformisation, steady-state probabilities

• Extensions: Costs & rewards
Rewards (or costs)

- Like DTMCs, we can augment CTMCs with rewards
  - real-valued quantities assigned to states and/or transitions
  - can be interpreted in two ways: instantaneous/cumulative
  - properties considered here: expected value of rewards
  - formal property specifications in an extension of CSL

- For a CTMC \((S,s_{\text{init}},R,L)\), a reward structure is a pair \((\rho,\iota)\)
  - \(\rho : S \to \mathbb{R}_{\geq 0}\) is a vector of state rewards
  - \(\iota : S \times S \to \mathbb{R}_{\geq 0}\) is a matrix of transition rewards

- For cumulative reward–based properties of CTMCs
  - state rewards interpreted as rate at which reward gained
  - if the CTMC remains in state \(s\) for \(t \in \mathbb{R}_{>0}\) time units, a reward of \(t \cdot \rho(s)\) is acquired
• Example: “size of message queue”
  - $\rho(s_i) = i$ and $\iota(s_i,s_j) = 0 \ \forall \ i,j$

• Example: “time for which queue is not full”
  - $\rho(s_i) = 1$ for $i < 3$, $\rho(s_3) = 0$ and $\iota(s_i,s_j) = 0 \ \forall \ i,j$
Reward structures – Examples

- Example: “number of requests served”

\[ \rho = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad \text{and} \quad \xi = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \]
CSL and rewards

- **PRISM extends CSL to incorporate reward-based properties**
  - adds R operator like the one added to PCTL

\[
\phi ::= \ldots \mid R_{\sim r} [ I^=t ] \mid R_{\sim r} [ C^{\leq t} ] \mid R_{\sim r} [ F \phi ] \mid R_{\sim r} [ S ]
\]

- expected reward is \( \sim r \)
  - “instantaneous”
  - “cumulative”
  - “reachability”
  - “steady-state”

- where \( r, t \in \mathbb{R}_{\geq 0}, \sim \in \{<,>,\leq,\geq\} \)

- \( R_{\sim r} [ \cdot ] \) means “the expected value of \( \cdot \) satisfies \( \sim r \)”
Types of reward formulae

• **Instantaneous**: $R_{\sim r} [ I=t ]$
  – the expected value of the reward at time-instant $t$ is $\sim r$
  – “the expected queue size after 6.7 seconds is at most 2”

• **Cumulative**: $R_{\sim r} [ C \leq t ]$
  – the expected reward cumulated up to time-instant $t$ is $\sim r$
  – “the expected requests served within the first 4.5 seconds of operation is less than 10”

• **Reachability**: $R_{\sim r} [ F \phi ]$
  – the expected reward cumulated before reaching $\phi$ is $\sim r$
  – “the expected requests served before the queue becomes full”

• **Steady-state** $R_{\sim r} [ S ]$
  – the long-run average expected reward is $\sim r$
  – “expected long-run queue size is at least 1.2”
Reward properties in PRISM

• **Quantitative form:**
  - e.g. $R = ? \left[ C \leq t \right]$  
  - what is the expected reward cumulated up to time-instant $t$?

• **Add labels to $R$ operator to distinguish between multiple reward structures defined on the same CTMC**
  - e.g. $R_{\text{num}\_\text{req} = ?} \left[ C \leq 4.5 \right]$  
  - “the expected number of requests served within the first 4.5 seconds of operation”
  - e.g. $R_{\text{pow} = ?} \left[ C \leq 4.5 \right]$  
  - “the expected power consumption within the first 4.5 seconds of operation”
Reward formula semantics

- **Formal semantics of the four reward operators:**

  - $s \models R_{=r}[I=t] \iff \text{Exp}(s, X_{I=t}) \sim r$
  - $s \models R_{\leq r}[C\leq t] \iff \text{Exp}(s, X_{C\leq t}) \sim r$
  - $s \models R_{\geq r}[F \Phi] \iff \text{Exp}(s, X_{F \Phi}) \sim r$
  - $s \models R_{\sim r}[S] \iff \lim_{t \to \infty} \left( \frac{1}{t} \cdot \text{Exp}(s, X_{C\leq t}) \right) \sim r$

- **where:**
  - $\text{Exp}(s, X)$ denotes the **expectation** of the random variable $X : \text{Path}(s) \to \mathbb{R}_{\geq 0}$ with respect to the **probability measure** $Pr_s$
Reward formula semantics

- Definition of random variables:

  - path $\omega = s_0 t_0 s_1 t_1 s_2 \ldots$
    - $\text{state of } \omega \text{ at time } t$
  
  - $X_{t=k}(\omega) = \rho(\omega @ t)$
    - $\text{time spent in state } s_i$
  
  - $X_{C_{st}}(\omega) = \sum_{i=0}^{j_t-1} \left( t_i \cdot \rho(s_i) + \mu(s_i, s_{i+1}) \right) + \left( t - \sum_{i=0}^{j_t-1} t_i \right) \cdot \rho(s_{j_t})$
    - $\text{time spent in state } s_{j_t} \text{ before } t \text{ time units have elapsed}$

  - $X_{F_\phi}(\omega) = \begin{cases} 
  0 & \text{if } s_0 \in \text{Sat}(\phi) \\
  \infty & \text{if } s_i \notin \text{Sat}(\phi) \text{ for all } i \geq 0 \\
  \left( \sum_{i=0}^{k_\phi-1} t_i \cdot \rho(s_i) + \mu(s_i, s_{i+1}) \right) & \text{otherwise}
  \end{cases}$

  - where $j_t = \min \{ j \mid \sum_{i \leq j} t_i \geq t \}$ and $k_\phi = \min \{ i \mid s_i \models \phi \}$
Model checking reward formulae

- **Instantaneous**: $R_{\sim r} [ I = t ]$
  - reduces to transient analysis (state of the CTMC at time $t$)
  - use uniformisation

- **Cumulative**: $R_{\sim r} [ C \leq t ]$
  - extends approach for time-bounded until
  - based on uniformisation

- **Reachability**: $R_{\sim r} [ F \phi ]$
  - can be computed on the embedded DTMC
  - reduces to solving a system of linear equations

- **Steady-state**: $R_{\sim r} [ S ]$
  - similar to steady state formulae $S_{\sim r} [ \phi ]$
  - graph based analysis (compute BSCCs)
  - solve systems of linear equations (compute steady state probabilities of each BSCC)
Summary

• Exponential distribution
  – suitable for modelling failures, waiting times, reactions, ...
  – nice mathematical properties

• Continuous–time Markov chains
  – transition delays modelled as exponential distributions
  – probability space over paths

• CSL: Continuous Stochastic Logic
  – extension of PCTL for properties of CTMCs

• CSL model checking
  – extension of PCTL model checking for DTMCs
  – uniformisation: efficient iterative method for transient prob.s

• Tomorrow: Probabilistic model checking in practice
  – PRISM, tool demo, counterexamples, bisimulation