Lecture 15
Long–run properties of DTMCs and MDPs

Dr. Dave Parker

Department of Computer Science
University of Oxford
Overview

• LTL – Linear temporal logic

• Repeated reachability and persistence

• Long–run properties of DTMCs
  − bottom strongly connected components (BSCCs)

• Long–run properties of MDPs
  − end components (E.C.s)
Limitations of PCTL

- PCTL, although useful in practice, has limited expressivity
  - essentially: probability of reaching states in $X$, passing only through states in $Y$ (and within $k$ time-steps)

- More expressive logics can be used, for example:
  - LTL [Pnu77] – the non-probabilistic linear-time temporal logic
  - PCTL* [ASB+95,BdA95] – which subsumes both PCTL and LTL
  - both allow path operators to be combined

- In PCTL, temporal operators always appear inside $P_{\sim p} […]$
  - (and, in CTL, they always appear inside $A$ or $E$)
  - in LTL (and PCTL*), temporal operators can be combined
Review – CTL and PCTL

• CTL:

- $\phi ::= \text{true} \mid a \mid \phi \land \phi \mid \neg \phi \mid A \psi \mid E \psi$
- $\psi ::= X \phi \mid \phi U \phi$

• PCTL

- $\phi ::= \text{true} \mid a \mid \phi \land \phi \mid \neg \phi \mid P_{\sim p} [ \psi ]$
- $\psi ::= X \phi \mid \phi U^{\leq k} \phi \mid \phi U \phi$

• Notation for paths: $\omega = s_0s_1s_2...$
  - Path(s) = set of all (infinite) paths with $s_0 = s$
  - $\omega(i)$ denotes the (i+1)th state, i.e. $\omega(i) = s_i$
  - $\omega[i...]$ is the suffix starting from $s_i$, i.e. $\omega[i...] = s_is_{i+1}s_{i+2}...$
LTL – Linear temporal logic

• LTL syntax
  – path formulae only
  – $\psi ::= \mathtt{true} \mid a \mid \psi \land \psi \mid \neg \psi \mid X \psi \mid \psi U \psi$
  – where $a \in \mathtt{AP}$ is an atomic proposition

• LTL semantics (for a path $\omega$)
  – $\omega \models \mathtt{true}$ always
  – $\omega \models a$ $\iff a \in \mathcal{L}(\omega(0))$
  – $\omega \models \psi_1 \land \psi_2$ $\iff \omega \models \psi_1$ and $\omega \models \psi_2$
  – $\omega \models \neg \psi$ $\iff \omega \not\models \psi$
  – $\omega \models X \psi$ $\iff \omega[1...] \models \psi$
  – $\omega \models \psi_1 U \psi_2$ $\iff \exists k \geq 0$ s.t. $\omega[k...] \models \psi_2$ and $\forall i < k \omega[i...] \models \psi_1$
LTL – Linear temporal logic

- Derived operators like CTL, for example:
  - $F \psi \equiv true \land U \psi$
  - $G \psi \equiv \neg F(\neg \psi)$

- LTL semantics (non-probabilistic)
  - implicit universal quantification over paths
  - i.e. for an LTS $M = (S, s_{init}, \rightarrow, L)$ and LTL formula $\psi$
  - $s \models \psi$ iff $\omega \models \psi$ for all paths $\omega \in \text{Path}(s)$
  - $M \models \psi$ iff $s_{init} \models \psi$

- e.g:
  - $A F (req \land X ack)$
  - “it is always possible that a request, followed immediately by an acknowledgement, can occur”
More LTL examples

- \((F \text{ tmp}\_\text{fail}_1) \land (F \text{ tmp}\_\text{fail}_2)\)
  - “both servers suffer temporary failures at some point”

- GF ready
  - “the server always eventually returns to a ready-state”

- G (req → F ack)
  - “requests are always followed by an acknowledgement”

- FG stable
  - “the system reaches and stays in a ‘stable’ state”
Branching vs. Linear time

• **LTL but not CTL:**
  - FG stable
  - “the system reaches and stays in a ‘stable’ state”
  - e.g. $A \text{ FG stable} \neq AF \text{ AG stable}$

• **CTL but not LTL:**
  - AG EF init
  - e.g. “for every computation, it is always possible to return to the initial state”
LTL + probabilities

• Same idea as PCTL: probabilities of sets of path formulae
  – for a state s of a DTMC and an LTL formula ψ:
  – \( \text{Prob}(s, \psi) = \Pr_s \{ \omega \in \text{Path}(s) \mid \omega \models \psi \} \)
  – all such path sets are measurable (see later lecture)

• For MDPs, we can again consider lower/upper bounds
  – \( p_{\text{min}}(s, \psi) = \inf_{\sigma \in \text{Adv}} \text{Prob}^\sigma(s, \psi) \)
  – \( p_{\text{max}}(s, \psi) = \sup_{\sigma \in \text{Adv}} \text{Prob}^\sigma(s, \psi) \)
  – (for LTL formula ψ)

• For DTMCs or MDPs, an LTL specification often comprises an LTL (path) formula and a probability bound
  – e.g. \( P_{>0.99} \{ F ( \text{req} \land X \text{ack} ) \} \)
PCTL*

• PCTL* subsumes both (probabilistic) LTL and PCTL

• State formulae:
  - $\phi ::= \text{true} \mid a \mid \phi \land \phi \mid \neg \phi \mid P_{\sim p} [ \psi ]$
  - where $a \in \text{AP}$, $\sim \in \{<,>,\leq,\geq\}$, $p \in [0,1]$ and $\psi$ a path formula

• Path formulae:
  - $\psi ::= \phi \mid \psi \land \psi \mid \neg \psi \mid X \psi \mid \psi U \psi$
  - where $\phi$ is a state formula

• A PCTL* formula is a state formula $\phi$
  - e.g. $P_{>0.99} [ GF \text{ crit}_1 ] \land P_{>0.99} [ GF \text{ crit}_2 ]$
  - e.g. $P_{\geq0.75} [ GF \text{ P}_{>0} [ F \text{ init } ]$
Fundamental property of DTMCs

- **Strongly connected component (SCC)**
  - maximally strongly connected set of states

- **Bottom strongly connected component (BSCC)**
  - SCC $T$ from which no state outside $T$ is reachable from $T$

- With probability 1, a BSCC will be reached and all of its states visited infinitely often

- Formally:
  \[
  \text{Pr}_s \{ \omega \in \text{Path}(s) \mid \exists \ i \geq 0, \exists \text{ BSCC } T \text{ such that } \\
  \forall \ j \geq i \ \omega(i) \in T \text{ and } \\
  \forall \ s' \in T \ \omega(k) = s' \text{ for infinitely many } k \} = 1
  \]
Repeated reachability – DTMCs

• Repeated reachability:
  – “always eventually…” or “infinitely often…”

• e.g. “what is the probability that the protocol successfully sends a message infinitely often?”

• Using LTL notation:
  – $\omega \models GF\ a$
    \[\iff\]
    – $\forall \ i \geq 0 . \ \exists \ j \geq i . \ \omega(j) \in Sat(a)$

• $\text{Prob}(s, GF\ a)$
  \[= \Pr_s \{ \omega \in \text{Path}(s) | \ \forall \ i \geq 0 . \ \exists \ j \geq i . \ \omega(j) \in Sat(a) \} \]
Qualitative repeated reachability

- $\Pr_s \{ \omega \in \text{Path}(s) \mid \forall i \geq 0 . \exists j \geq i . \omega(j) \in \text{Sat}(a) \} = 1$
- $P_{\geq 1} [ \text{GF } a ]$

if and only if

- $T \cap \text{Sat}(a) \neq \emptyset$ for all BSCCs $T$ reachable from $s$

Examples:

$s_0 \models P_{\geq 1} [ \text{GF } (b \lor c) ]$
$s_0 \not\models P_{\geq 1} [ \text{GF } b ]$
$s_2 \models P_{\geq 1} [ \text{GF } c ]$
Quantitative repeated reachability

- \[ \text{Prob}(s, \text{GF } a) = \text{Prob}(s, F T_{\text{GFA}}) \]
  - where \( T_{\text{GFA}} = \text{union of all BSCCs } T \text{ with } T \cap \text{Sat}(a) \neq \emptyset \)

Example:

\[ \text{Prob}(s_0, \text{GF } b) = \text{Prob}(s_0, F T_{\text{GFB}}) = \text{Prob}(s_0, F (T_1 \cup T_2)) = \text{Prob}(s_0, F \{s_3, s_4\}) = 2/3 + 1/6 = 5/6 \]

- From the above, we also have:
  - \( P_{>0} [ \text{GF } a ] \iff T \cap \text{Sat}(a) \neq \emptyset \text{ for some reachable BSCC } T \)
Persistence – DTMCs

• Persistence properties: “eventually always…”
  – e.g. “what is the probability of the leader election algorithm reaching, and staying in, a stable state?”
  – e.g. “what is the probability that an irrecoverable error occurs?”

• Using LTL notation:
  – $\omega \models FG a$
    $\iff$
  – $\exists i \geq 0 . \forall j \geq i . \omega(j) \in \text{Sat}(a)$

• $\text{Prob}(s, FG a)$
  $= Pr_s \{ \omega \in \text{Path}(s) \mid \exists i \geq 0 . \forall j \geq i . \omega(j) \in \text{Sat}(a) \}$
Qualitative persistence

- \( \Pr_s \{ \omega \in \text{Path}(s) \mid \exists \ i \geq 0 . \ \forall \ j \geq i . \ \omega(j) \in \text{Sat}(a) \} = 1 \)
- \( P_{\geq1} [ \text{FG} \ a ] \)

if and only if

- \( T \subseteq \text{Sat}(a) \) for all BSCCs \( T \) reachable from \( s \)

Examples:

\[
\begin{align*}
\ s_0 \not\models P_{\geq1} [ \text{FG} (b \lor c) ] \\
\ s_0 \models P_{\geq1} [ \text{FG} (b \lor c \lor d) ] \\
\ s_2 \models P_{\geq1} [ \text{FG} (c \lor d) ] \\
\end{align*}
\]
Quantitative persistence

- $\text{Prob}(s, \text{FG } a) = \text{Prob}(s, F T_{\text{FGa}})$
  - where $T_{\text{FGa}} = \text{union of all BSCCs } T$ with $T \subseteq \text{Sat}(a)$

Example:

$\text{Prob}(s_0, \text{FG } (b \lor c))$
$= \text{Prob}(s_0, F T_{\text{FG(b\lor c)}})$
$= \text{Prob}(s_0, F (T_1 \cup T_2))$
$= \text{Prob}(s_0, F \{s_3, s_4\})$
$= 2/3 + 1/6 = 5/6$
Success sets

- The sets $T_P$ for property $P$ are called success sets

  - $T_{\text{GFa}} = \text{union of all BSCCs } T \text{ with } T \cap \text{Sat}(a) \neq \emptyset$
  - $T_{\text{FGa}} = \text{union of all BSCCs } T \text{ with } T \subseteq \text{Sat}(a)$

- Sometimes denoted $U_P$
  - e.g. $U_{\text{GFa}}$
  - we use $T_P$ here (to avoid confusion with the until operator)
Repeated reachability + persistence

- Repeated reachability and persistence are dual properties
  - $GF\ a \equiv \neg(FG\ \neg a)$
  - $FG\ a \equiv \neg(GF\ \neg a)$
- Hence, for example:
  - $Prob(s, GF\ a) = 1 - Prob(s, FG\ \neg a)$

- Can show this through LTL equivalences, or...

- $Prob(s, GF\ a) + Prob(s, FG\ \neg a)$
  $= Prob(s, F\ T_{GFa}) + Prob(s, F\ T_{FG\neg a})$
  $= Prob(s, F\ (T_{GFa} \cup T_{FG\neg a})) = 1$ (fundamental DTMC property)
End components of MDPs

• Consider an MDP $M = (S, s_{init}, \text{Steps}, L)$

• A sub-MDP of $M$ is a pair $(T, \text{Steps}')$ where:
  – $T \subseteq S$ is a (non-empty) subset of $M$’s states
  – $\text{Steps}'(s) \subseteq \text{Steps}(s)$ for each $s \in T$
  – $(T, \text{Steps}')$ is closed under probabilistic branching, i.e. the set of states
    $\{ s' \mid \mu(s') > 0 \text{ for some } (a, \mu) \in \text{Steps}'(s) \}$
    is a subset of $T$

• An end component of $M$ is a strongly connected sub-MDP

Note:
• action labels omitted
• probabilities omitted where $=1$
End components – Examples

- **Sub-MDPs**
  - can be formed from state sets such as:
    - \{s_2, s_5, s_7, s_8\}, \{s_0, s_2, s_5, s_7, s_8\}, \{s_5, s_7, s_8\},
    - \{s_1, s_3, s_4\}, \{s_1, s_3, s_4, s_6\}, \{s_3, s_4\}, ...

- **End components**
  - can be formed from state sets:
    - \{s_3, s_4\}, \{s_1, s_3, s_4\}, \{s_6\}, \{s_5, s_7, s_8\}

- **Note that**
  - state sets do not necessarily uniquely identify end components
    - e.g. \{s_1, s_3, s_4\}
End components of MDPs

• For finite MDPs…
  – (analogue of fundamental property of finite DTMCs)

• For every end component, there is an adversary which, with probability 1, forces the MDP to remain in the end component, and visit all its states infinitely often

• Under every adversary $\sigma$, with probability 1 an end component will be reached and all of its states visited infinitely often
Repeated reachability – MDPs (max)

- Repeated reachability (GF) for MDPs
  - consider first the case of maximum probabilities...
  - $p_{\text{max}}(s, \text{GF } a)$

- First, a simple qualitative property:
  - $\text{Prob}^\sigma(s, \text{GF } a) > 0$ for some adversary $\sigma$, i.e. $p_{\text{max}}(s, \text{GF } a) > 0$
    $\iff$
    - $T \cap \text{Sat}(a) \neq \emptyset$ for some end component $T$ reachable from $s$

- The quantitative case (for maximum probabilities):
  - $p_{\text{max}}(s, \text{GF } a) = p_{\text{max}}(s, \text{F } T_{\text{GF}a})$
  - where $T_{\text{GF}a}$ is the union of sets $T$ for all end components $(T, \text{Steps'})$ with $T \cap \text{Sat}(a) \neq \emptyset$ (i.e. at least one $a$–state in $T$)
Example

- **Check:** $P_{<0.8} \ [ GF \ b ]$ for $s_0$

- **Compute** $p_{\text{max}}(GF \ b)$
  - $p_{\text{max}}(GF \ b) = p_{\text{max}}(s, F T_{GFb})$
  - $T_{GFb}$ is the union of sets $T$ for all end components with $T \cap \text{Sat}(b) \neq \emptyset$
  - $\text{Sat}(b) = \{ s_4, s_6 \}$
  - $T_{GFb} = T_1 \cup T_2 \cup T_3 = \{ s_1, s_3, s_4, s_6 \}$
  - $p_{\text{max}}(s, F T_{GFb}) = 0.75$
  - $p_{\text{max}}(GF \ b) = 0.75$

- **Result:** $s_0 \models P_{<0.8} \ [ GF \ b ]$
Repeated reachability – MDPs (max)

- **Quantitative case:**
  \[ p_{\text{max}}(s, \text{GF} \ a) = p_{\text{max}}(s, F T_{\text{G}a}) \]

- **This yields the qualitative property given earlier:**
  \[ \text{Prob}^\sigma(s, \text{GF} \ a) > 0 \text{ for some adversary } \sigma \]
  \[ \iff p_{\text{max}}(s, \text{GF} \ a) > 0 \]
  \[ \iff p_{\text{max}}(s, F T_{\text{G}a}) > 0 \]
  \[ \iff \text{Prob}^\sigma(s, F T_{\text{G}a}) > 0 \text{ for some adversary } \sigma \]
  \[ \iff s \models EF T_{\text{G}a} \]
  \[ \iff T \cap \text{Sat}(a) \neq \emptyset \text{ for some E.C. T reachable from } s \]

- **Another qualitative property:**
  \[ \text{Prob}^\sigma(s, \text{GF} \ a) = 1 \text{ for some adversary } \sigma \]
  \[ \iff p_{\text{max}}(s, \text{GF} \ a) = 1 \]
  \[ \iff p_{\text{max}}(s, F T_{\text{G}a}) = 1 \]

Compute with Prob1E
Repeated reachability – MDPs (min)

- Repeated reachability for MDPs – **minimum** probabilities
  - \( p_{\text{min}}(s, \text{GF a}) \)

- First, a useful qualitative property:
  - \( \text{Prob}^\sigma(s, \text{GF a}) = 1 \) for all adversaries \( \sigma \)
  - \( s \models P \geq 1 [ \text{GF a} ] \)
  - \( T \cap \text{Sat}(a) \neq \emptyset \) for all end components \( T \) reachable from \( s \)
Examples

- \( s_0 \models P_{\geq 1} [ GF (b \lor c \lor d) ] \)?

- \( s_0 \models P_{\geq 1} [ GF (b \lor d) ] \)?
Repeated reachability – MDPs (min)

• Repeated reachability for MDPs – **minimum** probabilities
  – \( p_{\text{min}}(s, \text{GF } a) \)

• Quantitative case
  – use duality of min/max probabilities for MDPs
  – \( p_{\text{min}}(s, \psi) = 1 - p_{\text{max}}(s, \neg \psi) \)
  – e.g. \( p_{\text{min}}(s, \text{GF } a) = 1 - p_{\text{max}}(s, \text{FG} \neg a) \)

• So min probabilities for repeated reachability (GF)
  – can be computed as max probabilities for persistence (FG)
Persistence – MDPs

- **Persistence for MDPs**
  - \( p_{min}(s, \text{FG } a) \) or \( p_{max}(s, \text{FG } a) \)

- **Quantitative case – maximum probabilities**
  - \( p_{max}(s, \text{FG } a) = p_{max}(s, \text{F } T_{FGa}) \)
  - where \( T_{FGa} \) is the union of sets \( T \) for all end components \((T, \text{Steps}')\) with \( T \subseteq \text{Sat}(a) \) (i.e. all states in \( T \) satisfy \( a \))
Repeated reachability (again)

• We now have way a of computing minimum probabilities for repeated reachability (GF)

\[ p_{\text{min}}(s, \text{GF } a) = 1 - p_{\text{max}}(s, \text{FG} \neg a) = 1 - p_{\text{max}}(s, \text{F } T_{\text{FG} \neg a}) \]

– where \( T_{\text{FG} \neg a} \) is the union of sets \( T \) for all end components \((T, \text{Steps'})\) with \( T \subseteq S \setminus \text{Sat}(a) \)

– ie. \( T_{\text{FG} \neg a} \) is the union of sets \( T \) for all end components \((T, \text{Steps'})\) with \( T \cap \text{Sat}(a) = \emptyset \)

• Can also now show why:

\[ s \models P_{\geq 1} [ \text{GF } a ] \iff T \cap \text{Sat}(a) \neq \emptyset \text{ for all end components } T \text{ reachable from } s \]
Examples

• $s_0 \models P_{>0} [ GF d ]$?

• $s_0 \models P_{>0.3} [ GF d ]$?
Summing up... I

- LTL: path-based, path operators can be combined
- PCTL*: subsumes PCTL and LTL

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>non-probabilistic (LTSs)</th>
<th>probabilistic (DTMCs, MDPs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTL</td>
<td>Φ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LTL</td>
<td>Ψ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCTL</td>
<td>Φ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LTL + prob.</td>
<td>Prob(s, ψ)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCTL*</td>
<td>Φ</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Summing up... II

- **2 useful instances of LTL formulae:**
  - repeated reachability: $\text{GF } a$
  - persistence: $\text{FG } a$
- **DTMCs**
  - qualitative: properties of reachable BSCCs
  - quantitative: probability of reaching success set (BSCC set)
- **MDPs**
  - end components: MDP analogue of BSCCs
  - $p_{\text{max}}(s, \text{GF } a)$ – max. reachability of success set ($T \cap \text{Sat}(a) \neq \emptyset$)
  - $P_{\geq 1}[\text{GF } a]$ – reachability of end components
  - $p_{\text{min}}(s, \text{GF } a)$ – one minus max. prob. for dual property
  - $p_{\text{max}}(s, \text{FG } a)$ – max. reachability of success set ($T \subseteq \text{Sat}(a)$)
  - $p_{\text{min}}(s, \text{FG } a)$ – again, via dual property