Lecture 4
Probabilistic temporal logics

Dr. Dave Parker

Department of Computer Science
University of Oxford
Overview

• Temporal logic

• Non-probabilistic temporal logic
  – CTL

• Probabilistic temporal logic
  – PCTL = CTL + probabilities

• Qualitative vs. quantitative

• Linear-time properties
  – LTL, PCTL*
Temporal logic

- **Temporal logic**
  - formal language for specifying and reasoning about how the behaviour of a system changes over time
  - extends propositional logic with modal/temporal operators
  - one important use: representation of system properties to be checked by a model checker

- **Logics used in this course are probabilistic extensions of temporal logics devised for non–probabilistic systems**
  - So we revert briefly to (labelled) state–transition diagrams

![Diagram](image-url)
State–transition systems

- Labelled state–transition system (LTS) (or Kripke structure)
  - is a tuple \((S, s_{\text{init}}, \rightarrow, L)\) where:
    - \(S\) is a set of states ("state space")
    - \(s_{\text{init}} \in S\) is the initial state
    - \(\rightarrow \subseteq S \times S\) is the transition relation
    - \(L : S \rightarrow 2^{AP}\) is function labelling states with atomic propositions (taken from a set \(AP\))

- DTMC \((S, s_{\text{init}}, P, L)\) has underlying LTS \((S, s_{\text{init}}, \rightarrow, L)\)
  - where \(\rightarrow = \{ (s, s') \text{ s.t. } P(s, s') > 0 \}\)
Paths – some notation

• Path $\omega = s_0s_1s_2...$ such that $(s_i,s_{i+1}) \in \rightarrow$ for $i \geq 0$
  – we write $s_i \rightarrow s_{i+1}$ as shorthand for $(s_i,s_{i+1}) \in \rightarrow$

• $\omega(i)$ is the $(i+1)$th state of $\omega$, i.e. $s_i$

• $\omega[...i]$ denotes the (finite) prefix ending in the $(i+1)$th state
  – i.e. $\omega[...i] = s_0s_1...s_i$

• $\omega[i...]$ denotes the suffix starting from the $(i+1)$th state
  – i.e. $\omega[i...] = s_is_{i+1}s_{i+2}...$

• As for DTMCs, Path(s) = set of all infinite paths from s
CTL

• CTL – Computation Tree Logic
• Syntax split into state and path formulae
  – specify properties of states/paths, respectively
  – a CTL formula is a state formula

• State formulae:
  – $\phi ::= \text{true} \mid a \mid \phi \land \phi \mid \neg \phi \mid A \psi \mid E \psi$
  – where $a \in AP$ and $\psi$ is a path formula

• Path formulae
  – $\psi ::= X \phi \mid F \phi \mid G \phi \mid \phi U \phi$
  – where $\phi$ is a state formula

Some of these operators (e.g. $A$, $F$, $G$) are derivable...

$X = \text{“next”}$
$F = \text{“future”}$
$G = \text{“globally”}$
$U = \text{“until”}$
CTL semantics

- Intuitive semantics:
  - of quantifiers (A/E) and temporal operators (F/G/U)

EF red

EG red

E [ yellow U red ]

AF red

AG red

A [ yellow U red ]
CTL semantics

• Semantics of state formulae:
  – \( s \models \phi \) denotes “\( s \) satisfies \( \phi \)” or “\( \phi \) is true in \( s \)”

• For a state \( s \) of an LTS \((S,s_{\text{init}},\rightarrow,L)\):
  – \( s \models \text{true} \) always
  – \( s \models a \) \iff a \in L(s)
  – \( s \models \phi_1 \land \phi_2 \) \iff \( s \models \phi_1 \) and \( s \models \phi_2 \)
  – \( s \models \neg \phi \) \iff s \not\models \phi
  – \( s \models A \psi \) \iff \( \omega \models \psi \) for all \( \omega \in \text{Path}(s) \)
  – \( s \models E \psi \) \iff \( \omega \models \psi \) for some \( \omega \in \text{Path}(s) \)
CTL semantics

• Semantics of path formulae:
  – \( \omega \models \psi \) denotes “\( \omega \) satisfies \( \psi \)” or “\( \psi \) is true along \( \omega \)”

• For a path \( \omega \) of an LTS \( (S, s_{\text{init}}, \rightarrow, L) \):

  – \( \omega \models X \phi \) \iff \( \omega(1) \models \phi \)
  – \( \omega \models F \phi \) \iff \( \exists k \geq 0 \text{ s.t. } \omega(k) \models \phi \)
  – \( \omega \models G \phi \) \iff \( \forall i \geq 0 \ \omega(i) \models \phi \)
  – \( \omega \models \phi_1 U \phi_2 \) \iff \( \exists k \geq 0 \text{ s.t. } \omega(k) \models \phi_2 \text{ and } \forall i < k \ \omega(i) \models \phi_1 \)
CTL examples

• Some examples of satisfying paths:
  - $\omega_0 \models X \text{succ}$
  - $\omega_1 \models \neg \text{fail} \cup \text{succ}$

• Example CTL formulas:
  - $s_1 \models \text{try} \land \neg \text{fail}$
  - $s_1 \models E [ X \text{succ} ]$ and $s_1, s_3 \models A [ X \text{succ} ]$
  - $s_0 \models E [ \neg \text{fail} \cup \text{succ} ]$ but $s_0 \not\models A [ \neg \text{fail} \cup \text{succ} ]$
CTL examples

- **AG (¬(crit₁ ∧ crit₂))**
  - mutual exclusion

- **AG EF initial**
  - for every computation, it is always possible to return to the initial state

- **AG (request → AF response)**
  - every request will eventually be granted

- **AG AF crit₁ ∧ AG AF crit₂**
  - each process has access to the critical section infinitely often
CTL equivalences

• Basic logical equivalences:
  - false $\equiv \neg \text{true}$ (false)
  - $\phi_1 \lor \phi_2 \equiv \neg(\neg\phi_1 \land \neg\phi_2)$ (disjunction)
  - $\phi_1 \rightarrow \phi_2 \equiv \neg\phi_1 \lor \phi_2$ (implication)

• Path quantifiers:
  - $A\,\psi \equiv \neg E(\neg\psi)$
  - $E\,\psi \equiv \neg A(\neg\psi)$

• Temporal operators:
  - $F\,\phi \equiv \text{true} \lor \phi$
  - $G\,\phi \equiv \neg F(\neg\phi)$

For example:
$AG\,\phi \equiv \neg EF(\neg\,\phi)$
CTL – Alternative notation

• Some commonly used notation…

• Temporal operators:
  – $F \phi \equiv \diamond \phi$ (“diamond”)
  – $G \phi \equiv \square \phi$ (“box”)
  – $X \phi \equiv \circ \phi$

• Path quantifiers:
  – $A \psi \equiv \forall \psi$
  – $E \psi \equiv \exists \psi$

• Brackets: none/round/square
  – $AF \psi$
  – $A ( \psi_1 \cup \psi_2 )$
  – $A [ \psi_1 \cup \psi_2 ]$
PCTL

- **Temporal logic for describing properties of DTMCs**
  - PCTL = Probabilistic Computation Tree Logic [HJ94]
  - essentially the same as the logic pCTL of [ASB+95]

- **Extension of (non–probabilistic) temporal logic CTL**
  - key addition is probabilistic operator P
  - quantitative extension of CTL’s A and E operators

- **Example**
  - send → P_{\geq 0.95} [ F_{\leq 10} deliver ]
  - “if a message is sent, then the probability of it being delivered within 10 steps is at least 0.95”
PCTL syntax

- PCTL syntax:

\[ \phi ::= \text{true} \mid a \mid \phi \land \phi \mid \neg \phi \mid P_{\sim p} [ \psi ] \]  

(state formulae)

\[ \psi ::= X \phi \mid \phi U \leq k \phi \mid \phi U \phi \]  

(path formulae)

- where \( a \) is an atomic proposition, \( p \in [0,1] \) is a probability bound, \( \sim \in \{<,>,\leq,\geq\} \), \( k \in \mathbb{N} \)

- A PCTL formula is always a state formula

- path formulae only occur inside the P operator
PCTL semantics for DTMCs

• Semantics for non-probabilistic operators same as for CTL:
  – \( s \vDash \phi \) denotes “\( s \) satisfies \( \phi \)” or “\( \phi \) is true in \( s \)”
  – \( \omega \vDash \psi \) denotes “\( \omega \) satisfies \( \psi \)” or “\( \psi \) is true along \( \omega \)”

• For a state \( s \) of a DTMC \((S,s_{\text{init}},P,L)\):
  – \( s \vDash \text{true} \) always
  – \( s \vDash a \iff a \in L(s) \)
  – \( s \vDash \phi_1 \land \phi_2 \iff s \vDash \phi_1 \) and \( s \vDash \phi_2 \)
  – \( s \vDash \neg \phi \iff s \nvDash \phi \)

• For a path \( \omega \) of a DTMC \((S,s_{\text{init}},P,L)\):
  – \( \omega \vDash X \phi \iff \omega(1) \vDash \phi \)
  – \( \omega \vDash \phi_1 U^{\leq k} \phi_2 \iff \exists i \leq k \text{ such that } \omega(i) \vDash \phi_2 \)
  and \( \forall j<i, \omega(j) \vDash \phi_1 \)
  – \( \omega \vDash \phi_1 U \phi_2 \iff \exists k \geq 0 \text{ s.t. } \omega(k) \vDash \phi_2 \) and \( \forall i<k, \omega(i) \vDash \phi_1 \)

U^{\leq k} not in CTL (but could easily be added)
PCTL semantics for DTMCs

- **Semantics of the probabilistic operator $P$**
  - informal definition: $s \models P_{\neg p} [\psi]$ means that “the probability, from state $s$, that $\psi$ is true for an outgoing path satisfies $\neg p$”
  - example: $s \models P_{<0.25} [X \text{ fail}] \iff$ “the probability of atomic proposition fail being true in the next state of outgoing paths from $s$ is less than 0.25”
  - formally: $s \models P_{\neg p} [\psi] \iff \text{Prob}(s, \psi) \sim p$
  - where: $\text{Prob}(s, \psi) = \Pr_s \{ \omega \in \text{Path}(s) \mid \omega \models \psi \}$
PCTL equivalences for DTMCs

- **Basic logical equivalences:**
  - \( \text{false} \equiv \neg \text{true} \)
  - \( \phi_1 \lor \phi_2 \equiv \neg (\neg \phi_1 \land \neg \phi_2) \)
  - \( \phi_1 \rightarrow \phi_2 \equiv \neg \phi_1 \lor \phi_2 \)

- **Negation and probabilities**
  - e.g. \( \neg P_{>p} [\phi_1 U \phi_2] \equiv P_{\leq p} [\phi_1 U \phi_2] \)
Reachability and invariance

• Derived temporal operators, like CTL…

• Probabilistic reachability: \( P_{\sim p} [ F \phi ] \)
  – the probability of reaching a state satisfying \( \phi \)
  – \( F \phi \equiv \text{true} U \phi \)
  – “\( \phi \) is eventually true”
  – bounded version: \( F^{\leq k} \phi \equiv \text{true} U^{\leq k} \phi \)

• Probabilistic invariance: \( P_{\sim p} [ G \phi ] \)
  – the probability of \( \phi \) always remaining true
  – \( G \phi \equiv \neg (F \neg \phi) \equiv \neg (\text{true} U \neg \phi) \)
  – “\( \phi \) is always true”
  – bounded version: \( G^{\leq k} \phi \equiv \neg (F^{\leq k} \neg \phi) \)

strictly speaking, \( G \phi \) cannot be derived from the PCTL syntax in this way since there is no negation of path formulae
Derivation of $P_{\sim p} [G \phi]$ 

- In fact, we can derive $P_{\sim p} [G \phi]$ directly in PCTL...
PCTL examples

- \( P_{<0.05} \left[ F_{\text{err/total}>0.1} \right] \)
  - “with probability at most 0.05, more than 10% of the NAND gate outputs are erroneous?”
- \( P_{\geq0.8} \left[ F_{\leq k \text{ reply\_count}=n} \right] \)
  - “the probability that the sender has received \( n \) acknowledgements within \( k \) clock-ticks is at least 0.8”
- \( P_{<0.4} \left[ \neg \text{fail}_A \cup \text{fail}_B \right] \)
  - “the probability that component B fails before component A is less than 0.4”
- \( \neg \text{oper} \rightarrow \ P_{\geq1} \left[ F \left( P_{>0.99} \left[ G_{\leq100} \text{ oper} \right] \right) \right] \)
  - “if the system is not operational, it almost surely reaches a state from which it has a greater than 0.99 chance of staying operational for 100 time units”
PCTL and measurability

- All the sets of paths expressed by PCTL are measurable
  - i.e. are elements of the $\sigma$–algebra $\Sigma_{\text{Path}(s)}$
  - see for example [Var85] (for a stronger result in fact)

- Recall: probability space $(\text{Path}(s), \Sigma_{\text{Path}(s)}, \text{Pr}_s)$
  - $\Sigma_{\text{Path}(s)}$ contains cylinder sets $C(\omega)$ for all finite paths $\omega$ starting in $s$ and is closed under complementation, countable union

- Next $(X \phi)$
  - cylinder sets constructed from paths of length one

- Bounded until $(\phi_1 U^{\leq k} \phi_2)$
  - (finite number of) cylinder sets from paths of length at most $k$

- Until $(\phi_1 U \phi_2)$
  - countable union of paths satisfying $\phi_1 U^{\leq k} \phi_2$ for all $k \geq 0$
Qualitative vs. quantitative properties

- P operator of PCTL can be seen as a quantitative analogue of the CTL operators A (for all) and E (there exists)

- **Qualitative PCTL properties**
  - $P_{\sim p} [ \psi ]$ where $p$ is either 0 or 1

- **Quantitative PCTL properties**
  - $P_{\sim p} [ \psi ]$ where $p$ is in the range $(0,1)$

- $P_{>0} [ F \phi ]$ is identical to $EF \phi$
  - there exists a finite path to a $\phi$–state

- $P_{\geq 1} [ F \phi ]$ is (similar to but) weaker than $AF \phi$
  - a $\phi$–state is reached “almost surely”
  - see next slide…
Example: Qualitative/quantitative

- Toss a coin repeatedly until “tails” is thrown

- Is “tails” always eventually thrown?
  - CTL: $\text{AF} \, \text{“tails”}$
  - Result: false
  - Counterexample: $s_0s_1s_0s_1s_0s_1\ldots$

- Does the probability of eventually throwing “tails” equal one?
  - PCTL: $P_{\geq 1} [ \text{F “tails” } ]$
  - Result: true
  - Infinite path $s_0s_1s_0s_1s_0s_1\ldots$ has zero probability
Quantitative properties

- Consider a PCTL formula $P_{\neg p} [ \psi ]$
  - if the probability is unknown, how to choose the bound $p$?
- When the outermost operator of a PCTL formula is $\neg$
  - PRISM allows formulae of the form $P=? [ \psi ]$
  - “what is the probability that path formula $\psi$ is true?”
- Model checking is no harder: compute the values anyway
- Useful to spot patterns, trends
- Example
  - $P=? [ F \text{err/total}>0.1 ]$
  - “what is the probability that 10% of the NAND gate outputs are erroneous?”
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

- To introduce these logics, we return briefly again to non-probabilistic logics and models...
Branching vs. Linear time

• In CTL, temporal operators always appear inside A or E
  – in LTL, temporal operators can be combined

• LTL but not CTL:
  – F [ req \land X ack ]
  – “eventually a request occurs, followed immediately by an acknowledgement”

• CTL but not LTL:
  – AG EF initial
  – “for every computation, it is always possible to return to the initial state”
LTL

- **LTL syntax**
  - path formulae only
  \[
  \psi ::= \text{true} \mid a \mid \psi \land \psi \mid \neg \psi \mid X \psi \mid \psi U \psi
  \]
  - where \(a \in \text{AP}\) is an atomic proposition

- **LTL semantics (for a path \(\omega\))**
  - \(\omega \models \text{true}\) always
  - \(\omega \models a \iff a \in L(\omega(0))\)
  - \(\omega \models \psi_1 \land \psi_2 \iff \omega \models \psi_1 \text{ and } \omega \models \psi_2\)
  - \(\omega \models \neg \psi \iff \omega \not\models \psi\)
  - \(\omega \models X \psi \iff \omega[1\ldots] \models \psi\)
  - \(\omega \models \psi_1 U \psi_2 \iff \exists k \geq 0 \text{ s.t. } \omega[k\ldots] \models \psi_2 \text{ and } \forall i<k \omega[i\ldots] \not\models \psi_1\)
LTL

• LTL semantics
  – 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:
  – $A\ F\ [\ \text{req} \land X\ \text{ack}]$
  – “it is always the case that, eventually, a request occurs, followed immediately by an acknowledgement”

• Derived operators like CTL, for example:
  – $F\ \psi \equiv \text{true U } \psi$
  – $G\ \psi \equiv \neg F(\neg\psi)$
LTL + probabilities

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

• Examples (from DTMC lectures)…

• Repeated reachability: “always eventually…”
  – $\text{Prob}(s, \text{GF send})$
  – e.g. “what is the probability that the protocol successfully sends a message infinitely often?”

• Persistence properties: “eventually forever…”
  – $\text{Prob}(s, \text{FG stable})$
  – e.g. “what is the probability of the leader election algorithm reaching, and staying in, a stable state?”
PCTL*

- PCTL* subsumes both (probabilistic) LTL and PCTL

- **State formulae:**
  - $\phi ::= \text{true} \mid a \mid \phi \land \phi \mid \neg \phi \mid P_{\neg p} [ \psi ]$
  - where $a \in \text{AP}$ and $\psi$ is 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. $P_{>0.1} [ GF \text{ crit}_1 ] \land P_{>0.1} [ GF \text{ crit}_2 ]$
### Summing up…

- **Temporal logic:**
  - formal language for specifying and reasoning about how the behaviour of a system changes over time

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Temporal Logic</th>
<th>Time</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTL</td>
<td>$\Phi$</td>
<td>non-probabilistic</td>
<td>(e.g. LTSs)</td>
</tr>
<tr>
<td>LTL</td>
<td>$\psi$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCTL</td>
<td>$\Phi$</td>
<td>probabilistic</td>
<td>(e.g. DTMCs)</td>
</tr>
<tr>
<td>LTL + prob.</td>
<td>Prob($s, \psi$)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCTL*</td>
<td>$\Phi$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>