Program correctness
Branching-time temporal logics

Marcello Bonsangue
CTL

- **CTL = Computational Tree Logic**
  - the temporal combinators are under the immediate scope of the path quantifiers

- **Why CTL?** The truth of CTL formulas depends only on the current state and not on the current execution!

  **Benefit**: easy and efficient model checking
  **Disadvantages**: hard for describing individual path
The language

- **Path quantifiers** allows to speak about sets of executions.
  - The model of time is tree-like: many futures are possible from a given state

- **Inevitably** \( A \phi \)
  - from the current state all executions satisfy \( \phi \)

- **Possibly** \( E \phi \)
  - from the current state there exists an execution satisfying \( \phi \)
CTL - Syntax

\[ \phi ::= p_1 \mid p_2 \mid \ldots \]

\[ T \mid \bot \mid \neg \phi \mid \phi \land \phi \mid \phi \lor \phi \mid \phi \Rightarrow \phi \mid \]

\[ AX\phi \mid AF\phi \mid AG\phi \mid A[\phi \cup \phi] \mid \]

\[ EX\phi \mid EF\phi \mid EG\phi \mid E[\phi \cup \phi] . \]
CTL - Priorities

- Unary connectives bind most tightly
  - $\square \neg$, AG, EG, AF, EF, AX, and EX
- Next come $\land$, and $\lor$
- Finally come, AU and EU

Example:

$AGp_1 \Rightarrow EGp_2$ is not the same as $AG(p_1 \Rightarrow EGp_2)$
CTL - yes or no?

- Yes
  - EFE[p U q]
  - A[p U EF q]

- No
  - EF(p U q)
  - FG p

- Yes or no?
  - AG(p → A[p U (¬p ∧ A[¬p U q])])
  - AF[(p U q) ∧ (q U p)]
A is not G

- $A\phi$ states that all the executions starting from the current state will satisfy $\phi$
- $G\phi$ state that $\phi$ holds at every state of the execution considered

- $A$ and $E$ quantify over paths in a tree
- $G$ and $F$ quantify over positions along a given path in a tree
Combining $E$ and $F$ (I)

- $EF\phi$

  “it is possible that $\phi$ will hold in the future”
Combining E and F (II)

- $\text{EG} \phi = \text{E} \overrightarrow{\text{F}} \overrightarrow{\phi}$

“it is possible that $\phi$ will always hold”
Combining E and F (III)

- $AF\phi = \neg E \neg F \phi$

  “it is inevitable that $\phi$ will hold in the future”
Combining E and F (IV)

- $\text{AG}\phi = \neg EF \neg \phi$
  
  "$\phi$ is always true"

- In this case $\phi$ is an invariant, that is, a property that is true continuously
Example

- All executions starting from 0 satisfy AFEXerror
  Why? Because from 0 all executions traverse 1 and may go to 2

- There exists an execution which does not satisfy AFAXerror. Which one?
Examples

- $\text{AGESF}\phi$

Along every execution (A)
from every state (G)
it is possible (E)
that we will encounter a state (F)
satisfying $\phi$

that is, $\phi$ is always reachable
CTL - Satisfaction

Let $M = <S, \rightarrow, l>$ be a transition system with $l(s)$ the set of atomic propositions satisfied by a state $s \in S$.

Idea for a model: A CTL formula refers to a given state of a given transition system.

$\Box M, s \models \phi$ means "$\phi$ is true at state $s$"

We will define it by induction on the structure of $\phi$. 
CTL - Semantics (I)

- $M, s \models T$ for all $s$ in $S$
- $M, s \models p$ iff $p \in l(s)$
- $M, s \models \neg \phi$ iff not $M, s \models \phi$
- $M, s \models \phi_1 \land \phi_2$ iff $M, s \models \phi_1$ and $M, s \models \phi_2$
  
  \[ \vdots \]
  
  \[ \vdots \]
CTL - Semantics (II)

- \( M,s \models AX\phi \) iff for all \( s' \) such that \( s \rightarrow s' \) we have \( M,s' \models \phi \)

- \( M,s \models EX\phi \) iff there exists \( s' \) such that \( s \rightarrow s' \) and \( M,s' \models \phi \)
CTL - Semantics (III)

- $M, s \vDash AG \phi$ iff for all executions
  $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \ldots$ with
  $s = s_0$ we have $M, s_i \vDash \phi$

- $M, s \vDash EG \phi$ iff there exists an execution
  $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \ldots$ with
  $s = s_0$ and such that $M, s_i \vDash \phi$
CTL - Semantics (IV)

- $M, s \models \text{AF} \phi$ iff for all executions $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \ldots$ with $s = s_0$ there is $i$ such that $M, s_i \models \phi$

- $M, s \models \text{EF} \phi$ iff there exists an execution $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \ldots$ with $s = s_0$ and there is $i$ such that $M, s_i \models \phi$
CTL - Semantics (V)

- $M, s \models A[\phi_1 \lor \phi_2]$ iff for all executions $s \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \ldots$ there is $i$ such that $M, s_i \models \phi_2$ and for each $j < i$ $M, s_j \models \phi_1$

- $M, s \models E[\phi_1 \lor \phi_2]$ iff there exists an execution $s \rightarrow s_1 \rightarrow s_2 \rightarrow s_3 \ldots$ and there is $i$ such that $M, s_i \models \phi_2$ and for each $j < i$ $M, s_j \models \phi_1$
CTL equivalences

- **De Morgan-based**
  - $\neg AF\phi \equiv EG\neg \phi$
  - $\neg EF\phi \equiv AG\neg \phi$
  - $\neg AX\phi \equiv EX\neg \phi$

  X-self duality: on a path each state has a unique successor

- **Until reduction**
  - $AF\phi \equiv A[T U \phi]$
  - $EF\phi \equiv E[T U \phi]$
CTL: Adequate sets of connectives

- **Theorem**: The set of operators $T, \neg, \wedge, \{AX \text{ or } EX\}, \{EG, AF \text{ or } AU\}$, and $EU$ is adequate for CTL.

\[ A[\phi U \psi] \equiv \neg (E[\neg \psi U (\neg \phi \wedge \neg \psi)] \vee EG \neg \psi) \]
CTL: Weak until and release

Use LTL equivalence to define:

- $A[\phi R \psi] \equiv \neg E[\neg \phi U \neg \psi]$
- $E[\phi R \psi] \equiv \neg A[\neg \phi U \neg \psi]$

- $A[\phi W \psi] \equiv A[\psi R (\phi \lor \psi)]$
- $E[\phi W \psi] \equiv E[\psi R (\phi \lor \psi)]$
Other CTL equivalences

- $\text{EG} \phi \equiv \phi \land \text{EX EG} \phi$
- $\text{AG} \phi \equiv \phi \land \text{AX AG} \phi$
- $\text{AF} \phi \equiv \phi \lor \text{AX AF} \phi$
- $\text{EF} \phi \equiv \phi \lor \text{EX EF} \phi$
- $\text{A}[\phi \text{U} \psi] \equiv \psi \lor (\phi \land \text{AXA}[\phi \text{U} \psi])$
- $\text{E}[\phi \text{U} \psi] \equiv \psi \lor (\phi \land \text{EXE}[\phi \text{U} \psi])$
CTL* - Syntax

- State formulas (evaluated in states)
  \[ \phi ::= T \mid p \mid \neg \phi \mid \phi \land \phi \mid A\psi \mid E\psi \]

- Path formulas (evaluated along paths)
  \[ \psi ::= \phi \mid \neg \psi \mid \psi \land \psi \mid X\psi \mid F\psi \mid G\psi \mid \psi U\psi \]
Examples

- AGF\(\phi\)

  Along every execution (A) from every state (G) we will encounter a state (F) satisfying \(\phi\)

  that is, \(\phi\) is satisfied infinitely often
Let $M = \langle S, \rightarrow, l \rangle$ be a transition system with $l(s)$ the set of atomic propositions satisfied by a state $s \in S$.

**Idea for a model:** A formula of temporal logic refers to an instant $i$ of an execution $\pi$ of a transition system $M$.

$M, \pi, i \models \phi$ means

“$\phi$ is true at position $i$ of path $\pi$ of $M$”
Semantics (I)

- $M,\pi,i \models T$ always
- $M,\pi,i \models p$ iff $p \in l(\pi(i))$
- $M,\pi,i \models \neg \phi$ iff not $M,\pi,i \models \phi$
- $M,\pi,i \models \phi_1 \land \phi_2$ iff $M,\pi,i \models \phi_1$ and $M,\pi,i \models \phi_2$
Semantics (II)

- $M, \pi, i \models X\phi$ iff $M, \pi, i+1 \models \phi$
- $M, \pi, i \models F\phi$ iff there exists $i \leq j$ such that $M, \pi, j \models \phi$
- $M, \pi, i \models G\phi$ iff $M, \pi, j \models \phi$ for all $i \leq j$
- $M, \pi, i \models \phi_1 U \phi_2$ iff there exists $i \leq j$ such that $M, \pi, j \models \phi_2$ and for all $i \leq k < j$ we have $M, \pi, k \models \phi_1$
Semantics (III)

- \( M, \pi, i \models E\phi \) iff there exists \( \pi' \) such that \( \pi(0) \ldots \pi(i) = \pi'(0) \ldots \pi'(i) \) and \( M, \pi', i \models \phi \)

- \( M, \pi, i \models A\phi \) iff for all \( \pi' \) such that \( \pi(0) \ldots \pi(i) = \pi'(0) \ldots \pi'(i) \) we have \( M, \pi', i \models \phi \)
LTL and CTL ⊆ CTL*

- Semantically, an LTL formula $\phi$ is equivalent to the CTL* formula $A\phi$.

- CTL is a restricted fragment of CTL* with path formulas

$$\psi ::= X\phi \mid F\phi \mid G\phi \mid \phi \lor \phi$$

and the same state formulas as CTL*, i.e.

$$\phi ::= T \mid p \mid \neg\phi \mid \phi \land \phi \mid A\psi \mid E\psi$$
Expressivity

CTL*

CTL

LTL

$\phi_1$

$\phi_2$

$\phi_3$

$\phi_4$
In CTL but not in LTL

\[ \phi_1 = AG \ EF \ p \] in CTL

From any state we can always get to a state in which \( p \) holds

\[ M, s \models \phi_1 \] but \( M', s \not\models \phi_1 \)

- It cannot be expressed as LTL formula \( \phi \) because
  - All executions starting from \( s \) in \( M' \) are also executions starting from \( s \) in \( M \)
  - In CTL \( M, s \models \phi_1 \) but \( M', s \not\models \phi_1 \)
In CTL and in LTL

\[ \phi_2 = AG(p \Rightarrow AFq) \text{ in CTL} \]

and

\[ \phi_2 = G(p \Rightarrow Fq) \text{ in LTL} \]

“Any p is eventually followed by a q”
In LTL but not in CTL

$\phi_3 = GFp \Rightarrow Fq$ in LTL

“If $p$ holds infinitely often along a path, then there is a state in which $q$ holds”

Note: $FGp$ is different from $AFAGp$ since the first is satisfied in whereas the latter is not (starting from $s$).
Neither in CTL nor in LTL

$\phi_4 = E(GFp)$ in CTL*

“There is a path with infinitely many state in which p holds”

- Not expressible in LTL: Trivial
- Not expressible in CTL: very complex
Boolean combination of path in CTL

- CTL = CTL* but
  - Without boolean combination of path formulas
  - Without nesting of path formulas

- The first restriction is not real ...
  - $E[Fp \land Fq] \equiv EF[p \land EFq] \lor EF[q \land EFp]$
    - First p and then q or viceversa
More generally …

- $E[\neg(pUq)] \equiv E[\neg qU(\neg p \land \neg q)] \lor EG \neg q$
- $E[(p_1Uq_1) \land (p_2Uq_2)] \equiv E[(p_1 \land p_2)U(q_1 \land E[p_2Uq_2])]$
- $E[(p_2Uq_2)U(q_2 \land E[p_1Uq_1])]
- $E[Fp \land Gq] \equiv E[q U (p \land EG q)]$
- $E[\neg Xp] \equiv EX\neg p$
- $E[Xp \land Xq] \equiv EX(p \land q)$
- $E[Fp \land Xq] \equiv EX(q \land EFp)$

- $A[\phi] \equiv \neg E[\neg \phi]$
Past operators

<table>
<thead>
<tr>
<th>Analogues of</th>
<th>Previous</th>
<th>Since</th>
<th>Once</th>
<th>Historically</th>
</tr>
</thead>
<tbody>
<tr>
<td>P X neXt</td>
<td>S U Until</td>
<td>O F Future</td>
<td>H G Globally</td>
<td></td>
</tr>
</tbody>
</table>

- In LTL they do not add expressive power, but CTL they do!