Formale Systeme 2

Prof. Dr. Peter H. Schmitt
CTL

Computation Tree Logic
Motivating Example

Transition System
Motivating Example

Transition System

The Transition system \( T = (S, R, \nu) \) uses propositional variables \( n_1, n_2, t_1, t_2, c_1, c_2 \) with the intended meaning.

\[
\begin{align*}
    s \models n_i & \quad \text{iff in state } s \text{ agent } i \text{ is not trying} \\
    s \models t_i & \quad \text{iff in state } s \text{ agent } i \text{ is trying} \\
    s \models c_i & \quad \text{iff in state } s \text{ agent } i \text{ is in the critical section}
\end{align*}
\]
Motivating Example

Properties

safety  There is no state $s$ reachable from $s_0$ with $s \models c_1 \land c_2$.

liveness  Whenever an agent tries to enter the critical section it will eventually enter it.

non-blocking  An agent can always try to enter the critical section.

non-sequencing  It is not the case that the agent who first tried will first enter the critical section.

non-alternating  It is not the case that the two agents take alternate turns to the critical section.
Motivating Example

Properties

The safety property is obviously true. There is not even a state $s$ with $s \models c_1 \land c_2$

The non-blocking property can easily seen to be true. Likewise the absence of dead ends
Modified Transition System
The liveness property is now true.

But now the non-sequencing property is violated.
Transition Systems

Definition

Let PVar be a set of propositional atoms. A transition system $\mathcal{T} = (S, R, v)$ consists of

- a finite set $S$ of states with one distinguished initial state $s_0$,
- a binary relation $R$ and
- a function $v : S \times \text{PVar} \rightarrow \{1, 0\}$

such that for every $s \in S$ there is $s' \in S$ with $R(s, s')$.

From a technical point of view a transition system is just a Kripke structure, whose accessibility relation has no dead ends.
Computation Tree Logic (CTL)

Syntax

1. Any propositional variable $p \in \text{PVar}$ is a CTL formula.
2. If $F$, $G$ are CTL formulas then all propositional combinations are also CTL formulas, e.g., $\neg F$, $F \lor G$, $F \land G$, etc.
3. If $F$, $G$ are CTL formulas then also

$$\text{AX}F, \text{EX}F, \text{A}(F \text{ U } G) \text{ and } \text{E}(F \text{ U } G)$$

are CTL formulas.

**Note:** The temporal operators $\text{A}$, $\text{E}$ and $\text{X}$, $\text{U}$ always occur in pairs.
Let \((S, R, v)\) be a transition system.

A path through \((S, R, v)\) is an infinite sequence of states

\[ t_1, t_2, \ldots, t_n, t_{n+1}, \ldots \]

such that \(t_1\) is the initial state and for all \(n\) the relation \(R(t_n, t_{n+1})\) is true.
Let \( \mathcal{T} = (S, R, \nu) \) be a transition system.

\((\mathcal{T}, s) \models \phi\),

**read:** formula \( \phi \) is true in state \( s \) of \( \mathcal{T} \),

will be abbreviated as \( s \models \phi \).

1. \( g \models p \) iff \( \nu(g, p) = 1 \) (in case \( p \in \text{PVar} \))
2. \( g \models \neg \phi \) iff \( g \not\models \phi \)
3. \( g \models \phi_1 \land \phi_2 \) iff \( g \models \phi_1 \) and \( g \models \phi_2 \)
4. \( g \models \text{AX} \phi \) iff \( g_1 \models \phi \) is true for all \( g_1 \) with \( R(g, g_1) \)
5. \( g \models \text{EX} \phi \) iff \( g_1 \models \phi \) is true for at least one \( g_1 \) with \( R(g, g_1) \)
CTL
Semantics (continued)

6  \( g \models A(\phi_1 U \phi_2) \)  iff  for every path \( g_0, g_1, \ldots \) with \( g_0 = g \) there exists \( i \geq 0 \), such that \( g_i \models \phi_2 \) and \( g_j \models \phi_1 \) for all \( j \) with \( 0 \leq j < i \),

7  \( g \models E(\phi_1 U \phi_2) \)  iff  there is a path \( g_0, g_1, \ldots \) with \( g_0 = g \) and there is \( i \geq 0 \), such that \( g_i \models \phi_2 \) and \( g_j \models \phi_1 \) for all \( j \) satisfying \( 0 \leq j < i \),
Defined CTL Operators

Using $F$ and $G$ from LTL four new CTL operators can be defined:

\[
\begin{align*}
ua(\phi) & \equiv AF\phi \equiv A(1 U \phi) & \phi \text{ cannot be avoided} \\
re(\phi) & \equiv EF\phi \equiv E(1 U \phi) & \phi \text{ is reachable} \\
ofa(\phi) & \equiv EG\phi \equiv \neg A(1 U \neg \phi) & \text{once and for all} \\
aw(\phi) & \equiv AG\phi \equiv \neg E(1 U \neg \phi) & \text{always } \phi
\end{align*}
\]

8 $g \models AF\phi$ iff for every path $g_0, g_1, \ldots$ with $g_0 = g$
there exists $i \geq 0$, such that $g_i \models \phi$

9 $g \models EF\phi$ iff there is a path $g_0, g_1, \ldots$ with $g_0 = g$
and there exists $i \geq 0$, such that $g_i \models \phi$

10 $g \models EG\phi$ iff there is a path $g_0, g_1, \ldots$ with $g_0 = g$
such that $g_i \models \phi$ for all $i$

11 $g \models AG\phi$ iff for every path $g_0, g_1, \ldots$ with $g_0 = g$
and every $i$ it is true that $g_i \models \phi$
The following formulas are CTL tautologies:

1. **AG** $\phi \leftrightarrow \phi \land \text{AXAG} \phi$
2. **EG** $\phi \leftrightarrow \phi \land \text{EXEG} \phi$
3. **AF** $\phi \leftrightarrow \phi \land \text{AXAF} \phi$
4. **EF** $\phi \leftrightarrow \phi \land \text{EXEF} \phi$
5. **A(φ U ψ)** $\leftrightarrow \psi \lor (\phi \land \text{AXA}(\phi \text{ U } \psi))$
6. **E(φ U ψ)** $\leftrightarrow \psi \lor (\phi \land \text{EXE}(\phi \text{ U } \psi))$
CTL*
CTL* Formulas

There are two categories of CTL* formulas

- state formulas and
- path formulas.

1. any propositional variable is a state formula
2. if $F$, $G$ are state formulas, so are $\neg F$, $F \lor G$, $F \land G$, etc.,
3. if $F$ is a path formula, then $(AF)$, $(EF)$ are state formulas,
4. every state formula also is a path formula,
5. if $F$, $G$ are path formulas, so are $\neg F$, $F \lor G$, $F \land G$,
6. if $F$, $G$ are path formulas, so $XF$ und $F U G$. 
Comparative Expressive Power

LTL

CTL

CTL*

◦

A(GFp → Fq)

◦

AGEFp

◦

G(p → Fq)

AG(p → AFq)

◦

EAFp

Prof. Dr. Peter H. Schmitt – FM2
Comparing CTL* with LTL

Lemma

Let $F$ be a CTL* state formula. Then $F$ is expressible in LTL iff $F$ is equivalent to $\mathbf{A}(F^d)$.

$F^d$ denotes the formula that arises from $F$ by simply dropping all quantifiers. Thus e.g., $(\mathbf{AFA}Gp)^d = FGp$.

Proof: E.M.Clarke and I.A.Draghicescu, 1988
Comparing CTL with LTL

Application of previous Lemma

The formula $\phi = \text{AFAG} p$ is in CTL but not in LTL.

$\phi^d = \text{FG} p$

Set of all paths starting in $s_0$ is \{ $s_0^n s_1 s_3^\omega$ | $n \geq 1$ \} $\cup$ \{ $s_0^\omega$ \}.

$s_0 \models \text{AFG} p$ but $s_0 \not\models \text{AFAG} p$. 
Example reconsidered

Properties

safety  There is no state $s$ reachable from $s_0$ with
$s \models c_1 \land c_2$.
$s_1 \models \mathbf{AG} \neg (c_1 \land c_2)$

liveness  Whenever an agent tries it will eventually enter the CS.
$s_1 \models \mathbf{AG} (t_i \rightarrow \mathbf{A} (t_i \cup c_i))$

non-blocking  An agent can always try to enter the critical section.
$s_1 \models \mathbf{AG} (\neg (c_i \lor t_i) \rightarrow \mathbf{AX} t_i)$

non-sequencing  It is not the case that the agent who first tried will first enter the critical section.
$s_1 \models \neg \mathbf{AG} (t_1 \rightarrow \mathbf{A} ((t_1 \land \neg c_2) \cup c_1))$

non-alternating  It is not the case that the two agents take alternate turns to the critical section.
$s_1 \models \neg \mathbf{AG} (c_1 \rightarrow \mathbf{A} ((\neg c_1) \cup w c_2))$