CTL (Clarke & Emerson 81)

Definition: Semantics
All CTL-formulae are state formulae. Hence, we have a simpler semantics.
Let $M = (S, T, I, AP, l)$ be a Kripke structure without deadlocks and let $s \in S$.

- $M, s \models p$ if $p \in \ell(s)$
- $M, s \models \Box \varphi$ if $\forall x \to s'$ with $M, s' \models \varphi$
- $M, s \models \Diamond \varphi$ if $\exists x \to s'$ we have $M, s' \models \varphi$
- $M, s \models \Box \varphi$ if $\exists x = s_0 \to s_1 \to s_2 \cdots \to s_k$ finite path, with $M, s_1 \models \varphi$ and $M, s_j \models \varphi$ for all $0 \leq j < k$
- $M, s \models \Diamond \varphi$ if $\forall x = s_0 \to s_1 \to s_2 \cdots \cdots$ infinite paths, $\exists k \geq 0$ with $M, s_k \models \varphi$ and $M, s_j \models \varphi$ for all $0 \leq j < k$

Example:

- $[\exists x \, p] = \{1, 2, 3, 5, 6\}$
- $[\forall x \, p] = \{3\}$
- $[\Box x \, p] = \{1, 2, 3, 4, 5, 6, 7, 8\}$
- $[\Diamond x \, p] = \{2, 3, 5, 6, 7\}$
- $[\Box x \, q \, U \, r] = \{1, 2, 3, 4, 5, 6\}$
- $[\forall x \, q \, U \, r] = \{2, 3, 4, 5, 6\}$

Model checking of CTL

Definition: Existential and universal model checking
Let $M = (S, T, I, AP, l)$ be a Kripke structure and $\varphi \in CTL$ a formula.

- $M, s \models \varphi$ if $M, s \models \varphi$ for some $s \in I$.
- $M, s \models \varphi$ if $M, s \models \varphi$ for all $s \in I$.

Remark:

- $M \models \varphi$ if $I \cap \{s \mid \models \varphi\} \neq \emptyset$
- $M \models \varphi$ if $I \subseteq \{s \mid \models \varphi\}$
- $M \models \varphi$ if $M \models \varphi$

Definition: Model checking problems $MC^\exists_{CTL}$ and $MC^\forall_{CTL}$

Input: A Kripke structure $M = (S, T, I, AP, l)$ and a formula $\varphi \in CTL$.

Question: Does $M \models \varphi$? or Does $M \models \varphi$?

Theorem:
Let $M = (S, T, I, AP, l)$ be a Kripke structure and $\varphi \in CTL$ a formula. The model checking problem $M \models \varphi$ is decidable in time $O(|M| \cdot |\varphi|)$

References

Model checking of CTL

**Theorem**

Let $M = (S, T, I, AP, t)$ be a Kripke structure and $\varphi$ be CTL a formula. The model checking problem $M \models \varphi$ is decidable in time $O(|M| + |\varphi|)$.

**Proof:**

Compute $[\varphi] = \{s \in S \mid M, s \models \varphi\}$ by induction on the formula.

The set $[\varphi]$ is represented by a boolean array: $L[s][\varphi] = T$ if $s \in [\varphi]$.

The labelling $L$ is encoded in $L$: for $p \in AP$ we have $L[s][p] = T$ if $p \in t(s)$.

For each $t \in S$, the set $T^{-1}(t)$ is represented as a list.

for all $t \in S$ do for all $s \in T^{-1}(t)$ do ... od takes time $O(T)$.

**Model Checking of CTL**

**Definition: procedure semantics($\varphi$)**

\[
\begin{align*}
\text{case } \varphi &= E \varphi_1 U \varphi_2 \\
\quad &\quad \text{case } \varphi = \neg \varphi_1 \\
\quad &\quad \text{case } \varphi = \varphi_1 \lor \varphi_2 \\
\quad &\quad \text{case } \varphi = \varphi_1 \land \varphi_2 \\
\quad &\quad \text{case } \varphi = EX \varphi_1 \\
\text{Todo} &:= [\varphi_1] \quad \text{semantics}(\varphi_1) \\
\text{Good} &:= \text{semantics}(\varphi_2) \\
\text{while } \text{Todo} \neq 0 \text{ do } \\
\text{Invariant 1: } [\varphi_1] \cup \text{Todo} \subseteq \text{Good} \subseteq [E \varphi_1 U \varphi_2] \\
\text{Invariant 2: } [\varphi_1] \cap T^{-1}(\text{Good} \cup \text{Todo}) \subseteq \text{Good} \\
\text{take } t \in \text{Todo}; \text{Todo} := \text{Todo} \setminus \{t\} \\
\text{for all } s \in T^{-1}(t) \text{ do } \\
\text{if } s \in [\varphi_1] \text{ then } \\
\text{Todo} := \text{Todo} \cup \{s\}; \text{Good} := \text{Good} \cup \{s\} \\
\text{od} \\
\text{[\varphi] := Good} \\
\text{end while} \\
\text{Good is only used to make the invariant clear. It can be replaced by [\varphi].}
\end{align*}
\]

**Model Checking of CTL**

**Definition: procedure semantics($\varphi$)**

\[
\begin{align*}
\text{case } \varphi &= A \varphi_1 U \varphi_2 \\
\quad &\quad \text{case } \varphi = \neg \varphi_1 \\
\quad &\quad \text{case } \varphi = \varphi_1 \lor \varphi_2 \\
\quad &\quad \text{case } \varphi = \varphi_1 \land \varphi_2 \\
\quad &\quad \text{case } \varphi = EX \varphi_1 \\
\text{Todo} &:= [\varphi_1] \quad \text{semantics}(\varphi_1) \\
\text{Good} &:= \text{semantics}(\varphi_2) \\
\text{while } \text{Todo} \neq 0 \text{ do } \\
\text{Invariant 1: } [\varphi_1] \cup \text{Todo} \subseteq \text{Good} \subseteq [A \varphi_1 U \varphi_2] \\
\text{Invariant 2: } s \in S, c[s] = T(s) \text{ implies } [\varphi_1] \subseteq \{s\} \\
\text{Invariant 3: } [\varphi_1] \cap [s] \subseteq \text{Good} \\
\text{take } t \in \text{Todo}; \text{Todo} := \text{Todo} \setminus \{t\} \\
\text{for all } s \in T^{-1}(t) \text{ do } \\
\text{if } [s] \neq 0 \text{ and } s \in [\varphi_1] \text{ then } \\
\text{Todo} := \text{Todo} \cup \{s\}; \text{Good} := \text{Good} \cup \{s\} \\
\text{od} \\
\text{[\varphi] := Good} \\
\text{end while} \\
\text{Good is only used to make the invariant clear. It can be replaced by [\varphi].}
\end{align*}
\]

**Complexity of CTL**

**Definition:** SAT(CTL)

**Input:** A formula $\varphi$ in CTL

**Question:** Existence of a model $M$ and a state $s$ such that $M, s \models \varphi$?

**Theorem:** Complexity

- The model checking problem for CTL is PTIME-complete.
- The satisfiability problem for CTL is EXPTIME-complete.
Fairness

Example: Fairness

Only fair runs are of interest
- Each process is enabled infinitely often: $\bigwedge_i G F \text{run}_i$
- No process stays ultimately in the critical section: $\bigwedge_i \neg F G \text{CS}_i = \bigwedge_i G F \neg \text{CS}_i$

Definition: Fair Kripke structure

$M = (S, T, I, AP, \ell, F_1, \ldots, F_n)$ with $F_i \subseteq S$.

An infinite run $\sigma$ is fair if it visits infinitely often each $F_i$

Fair CTL

Definition: Syntax of fair-CTL

$\varphi ::= \bot \mid p \ (p \in AP) \mid \neg \varphi \mid \varphi \lor \varphi \mid EF X \varphi \mid AF X \varphi \mid EF \varphi U \psi \mid AF \varphi U \psi \mid Ef \parallel \varphi$

Definition: Semantics as a fragment of $\text{CTL}^*$

Let $M = (S, T, I, AP, \ell, F_1, \ldots, F_n)$ be a fair Kripke structure.

Then, $E_f \varphi = E(\text{fair} \land \varphi)$ and $A_f \varphi = A(\text{fair} \rightarrow \varphi)$

where $\text{fair} = \bigwedge_i G F \text{run}_i$

Model checking of $\text{CTL}_f$

Proof: Computation of $E_f X \varphi = E X (E_f \varphi)$

Proof: Computation of $A_f X \varphi = A X (E_f \varphi)$

Proof: Computation of $E_f \varphi U \psi = E \varphi U (E_f \varphi)$

Proof: Computation of $A_f \varphi U \psi = (\neg E_f G \neg \psi) \land \neg E_f (\neg \psi U (\neg \varphi \land \neg \psi))$

Hence, we only need to compute the semantics of $E_f G \varphi$.

Proof: Computation of $A_f G \varphi$

Let $M_{\varphi}$ be the restriction of $M$ to $[\varphi]_f$.

Compute the SCC of $M_{\varphi}$ with Tarjan’s algorithm (in linear time).

Let $S'$ be the union of the (non trivial) SCCs of $M_{\varphi}$ which intersect each $F_i$.

Then, $M, s \models E_f G \varphi$ iff $M_{\varphi}, s \models E \varphi U S'$ iff $M_{\varphi}, s \models EF S'$.

This is again a reachability problem which can be solved in linear time.