

3 Die Logik CTL

In diesem Kapitel betrachten wir – solange nicht explizit anders erwähnt – nur knotenbeschriftete, totale Transitionssysteme.

3.1 Syntax und Semantik

Definition 3.1

Sei \mathcal{P} eine Menge atomarer Propositionen. Formeln der *Computation Tree Logic* (CTL) sind gegeben durch folgende Grammatik.

$$\varphi ::= q \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \neg \varphi \mid \text{EX}\varphi \mid \text{AX}\varphi \mid \text{E}(\varphi\text{U}\psi) \mid \text{A}(\varphi\text{U}\psi) \mid \text{E}(\varphi\text{R}\psi) \mid \text{A}(\varphi\text{R}\psi)$$

wobei $q \in \mathcal{P}$.

Die einzelnen Operatoren werden gelesen als “*es gibt einen Lauf*” (E), “*für alle Läufe*” (A), “*next*” (X), “*until*” (U) und “*release*” (R).

Definition 3.2

Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ ein totales, knotenbeschriftetes Transitionssystem. Die Semantik einer CTL-Formel φ über \mathcal{T} ist induktiv definiert wie folgt. Seien $s, t, s_0, \dots, t_0, \dots \in \mathcal{S}$.

$$\begin{aligned} \mathcal{T}, s \models q & \text{ gdw. } q \in \lambda(s) \\ \mathcal{T}, s \models \varphi \vee \psi & \text{ gdw. } \mathcal{T}, s \models \varphi \text{ oder } \mathcal{T}, s \models \psi \\ \mathcal{T}, s \models \varphi \wedge \psi & \text{ gdw. } \mathcal{T}, s \models \varphi \text{ und } \mathcal{T}, s \models \psi \\ \mathcal{T}, s \models \neg \varphi & \text{ gdw. } \mathcal{T}, s \not\models \varphi \\ \mathcal{T}, s \models \text{EX}\varphi & \text{ gdw. } \exists t, s \rightarrow t \text{ und } \mathcal{T}, t \models \varphi \\ \mathcal{T}, s \models \text{AX}\varphi & \text{ gdw. } \forall t : \text{wenn } s \rightarrow t \text{ dann } \mathcal{T}, t \models \varphi \\ \mathcal{T}, s \models \text{E}(\varphi\text{U}\psi) & \text{ gdw. } \exists \text{ Lauf } s_0, s_1, \dots \text{ mit } s_0 = s \text{ und } \exists k \in \mathbb{N} \text{ mit } \mathcal{T}, s_k \models \psi \\ & \text{ und } \forall i < k : \mathcal{T}, s_i \models \varphi \\ \mathcal{T}, s \models \text{A}(\varphi\text{U}\psi) & \text{ gdw. } \forall \text{ Läufe } s_0, s_1, \dots \text{ mit } s_0 = s : \exists k \in \mathbb{N} \text{ mit } \mathcal{T}, s_k \models \psi \\ & \text{ und } \forall i < k : \mathcal{T}, s_i \models \varphi \\ \mathcal{T}, s \models \text{E}(\varphi\text{R}\psi) & \text{ gdw. } \exists \text{ Lauf } s_0, s_1, \dots \text{ mit } s_0 = s \text{ und } \forall k \in \mathbb{N} : \mathcal{T}, s_k \models \psi \\ & \text{ oder } \exists i < k : \mathcal{T}, s_i \models \varphi \\ \mathcal{T}, s \models \text{A}(\varphi\text{R}\psi) & \text{ gdw. } \forall \text{ Läufe } s_0, s_1, \dots \text{ mit } s_0 = s : \forall k \in \mathbb{N} : \mathcal{T}, s_k \models \psi \\ & \text{ oder } \exists i < k : \mathcal{T}, s_i \models \varphi \end{aligned}$$

Ist ein Transitionssystem \mathcal{T} und eine CTL-Formel φ gegeben, dann schreiben wir $\llbracket \varphi \rrbracket^{\mathcal{T}}$ für $\{s \mid \mathcal{T}, s \models \varphi\}$.

3 Die Logik CTL

Folgendes Lemma besagt, dass sich weder die Ausdrucksstärke noch die Prägnanz von CTL verändert, wenn Formeln nur in positiver Normalform, d.h. mit Negationssymbolen nur vor atomaren Propositionen, betrachtet werden.

Lemma 3.1

Es gelten die folgenden Äquivalenzen für alle $\varphi, \psi \in \text{CTL}$.

- a) $\neg \text{EX}\varphi \equiv \text{AX}\neg\varphi$,
- b) $\neg \text{E}(\varphi \text{U}\psi) \equiv \text{A}(\neg\varphi \text{R}\neg\psi)$,
- c) $\neg \text{A}(\varphi \text{U}\psi) \equiv \text{E}(\neg\varphi \text{R}\neg\psi)$,

Beweis Übung. ■

Satz 3.1

Über knoten-beschrifteten, totalen Transitionssystemen gilt: $\text{HML} \preceq \text{CTL}$.

Beweis (\leq) Leicht per Induktion über den Formelaufbau zu zeigen. Sei $\hat{\varphi}$ eine zu der HML-Formel äquivalente CTL-Formel. Dann gilt insbesondere: $\diamond\varphi \equiv \text{EX}\hat{\varphi}$ und $\Box\varphi \equiv \text{AX}\hat{\varphi}$.

(\neq) Im Beweis von Satz 2.7 wird gezeigt, dass keine HML-Formel die Eigenschaft “es gibt einen Pfad, auf dem irgendwann einmal φ gilt” ausdrückt, selbst wenn φ eine HML-Formel ist. Laut erstem Teil ist $\hat{\varphi}$ dann eine äquivalente CTL-Formel, und $\text{E}(\text{ttU}\hat{\varphi})$ beschreibt die gewünschte Eigenschaft. ■

Korollar 3.1

Das Model Checking Problem für CTL ist P-hart.

Satz 3.2

Sei \mathcal{T} ein Transitionssystem mit Zuständen s, t . Wenn $s \sim t$, dann gilt für alle $\varphi \in \text{CTL}$: $\mathcal{T}, s \models \varphi$ gdw. $\mathcal{T}, t \models \varphi$.

Beweis Genauso wie im Beweis von Satz 2.1 durch Induktion über den Formelaufbau. ■

3.2 Beispiele

Definition 3.3

Neben den üblichen Abkürzungen für den aussagenlogischen Teil von CTL definieren wir noch folgende Abkürzungen: $Q\text{F}\varphi := Q(\text{ttU}\varphi)$ (gelesen “*finally*” oder “*eventually*”) und $Q\text{G}\varphi := Q(\text{ffR}\varphi)$ (gelesen “*generally*” oder “*globally*”) – jeweils für $Q \in \{\text{E}, \text{A}\}$.

Beispiel 3.1

Ein paar CTL-Formeln und ihre intuitive Bedeutung.

Formel	Bedeutung
$\text{AG}\varphi$	überall gilt φ
$\text{AGEF}\varphi$	immer ist noch ein Zustand erreichbar, in dem φ gilt
$\text{AGAF}\varphi$	auf jedem Lauf gilt φ unendlich oft

Beispiel 3.2

Wir betrachten nochmals das Beispiel der Verkehrsampel aus Kapitel 1. Diese modellieren wir durch ein knotenbeschriftetes, totales Transitionssystem über den Propositionen $frot$, $fgruen$, $arot$, $arotgelb$, $agruen$, $agelb$ für die einzelnen Zustände der Fußgänger- und der Autofahrerampel, sowie einer Proposition $gedrueckt$, um zu signalisieren, dass ein Fußgänger die Straße kreuzen möchte. Die Ampelschaltung soll die folgenden Eigenschaften haben.

1. Zu Beginn und nur dann sind beide Ampeln rot.
2. Die Fussgängerampel ist entweder rot oder grün, die Autofahrerampel entweder rot, rotgelb, grün oder gelb.
3. Immer wenn die Autofahrerampel gelb ist, ist sie danach rot, und wenn sie rotgelb ist, ist sie danach grün.
4. Immer wenn einer der Ampeln grün ist, ist die andere rot.
5. Wenn die Fußgängerampel grün ist, ist sie im nächsten Schritt rot.
6. Immer wenn der Fußgängersignalknopf gedrückt ist, wird irgendwann danach die Fußgängerampel grün und der Signalkopf ist dann nicht mehr gedrückt. Bis dahin ist sie rot.
7. Der Signalknopf kann immer wieder gedrückt werden.

Dies kann man in CTL folgendermaßen ausdrücken. Sei $A := \{arot, arotgelb, agelb, agruen\}$.

$$\begin{aligned}
 \varphi_{Ampel} := & frot \wedge arot \wedge AXAG\neg(frot \wedge arot) \\
 & \wedge AG((fgruen \leftrightarrow \neg frot) \wedge (\bigvee_{q \in A} q) \wedge (\bigwedge_{p, q \in A, p \neq q} \neg(p \wedge q))) \\
 & \wedge AG((agelb \rightarrow AXarot) \wedge (arotgelb \rightarrow AXagruen)) \\
 & \wedge AG((fgruen \rightarrow arot) \wedge (agruen \rightarrow frot)) \\
 & \wedge AG(fgruen \rightarrow AXfrot) \\
 & \wedge AG(gedrueckt \rightarrow A(frot \cup (fgruen \wedge \neg gedrueckt))) \\
 & \wedge AGEFGedrueckt
 \end{aligned}$$

3.3 Entscheidungsverfahren und Komplexität

3.3.1 Fixpunktentwicklungen

Eine direkte Möglichkeit, Model Checking für CTL durchzuführen, ist direkt die Semantik einer Formel in einem Zustand auszuwerten. Für eine Formel der Form $EF\varphi$ z.B. betrachtet man alle aus diesem Zustand ausgehenden Läufe und testet, ob es unter diesen einen mit einer Position gibt, die φ erfüllt. Dies ist allerdings nicht nur sehr ineffizient,

3 Die Logik CTL

es ist auch auf Anhieb gar nicht klar, dass dies zu einem terminierenden Entscheidungsverfahren führt. Beachte, dass es selbst in einem endlichen Transitionssystem unendlich viele verschiedene Läufe geben kann.

Definition 3.4

Die *Unterformelmeng*e $Sub(\varphi)$ einer CTL-Formel φ ist wie üblich als die Menge aller Teilbäume des Syntaxbaums von φ definiert. Zudem betrachten wir noch die *erweiterte Unterformelmeng*e $Sub^*(\varphi)$, welche induktiv wie folgt definiert ist.

$$\begin{aligned}
Sub^*(q) &:= \{q\} \\
Sub^*(\varphi \vee \psi) &:= \{\varphi \vee \psi\} \cup Sub^*(\varphi) \cup Sub^*(\psi) \\
Sub^*(\varphi \wedge \psi) &:= \{\varphi \wedge \psi\} \cup Sub^*(\varphi) \cup Sub^*(\psi) \\
Sub^*(\neg\varphi) &:= \{\neg\varphi\} \cup Sub^*(\varphi) \\
Sub^*(QX\varphi) &:= \{QX\varphi\} \cup Sub^*(\varphi) \\
Sub^*(Q(\varphi U\psi)) &:= \{Q(\varphi U\psi), QXQ(\varphi U\psi), \varphi \wedge QXQ(\varphi U\psi), \psi \vee (\varphi \wedge QXQ(\varphi U\psi))\} \\
&\quad \cup Sub^*(\varphi) \cup Sub^*(\psi) \\
Sub^*(Q(\varphi R\psi)) &:= \{Q(\varphi R\psi), QXQ(\varphi R\psi), \varphi \vee QXQ(\varphi R\psi), \psi \wedge (\varphi \wedge QXQ(\varphi R\psi))\} \\
&\quad \cup Sub^*(\varphi) \cup Sub^*(\psi)
\end{aligned}$$

für $Q \in \{E, A\}$.

Lemma 3.2

Für alle $\varphi \in \text{CTL}$ gilt: $|Sub^*(\varphi)| \leq 4 \cdot |Sub(\varphi)|$.

Beweis Wiederum durch Induktion über den Formelaufbau von φ . ■

Im folgenden spielt die erweiterte Unterformelmeng

e eine wichtigere Rolle als die einfache Unterformelmenge.

Lemma 3.3

Für alle $\varphi, \psi \in \text{CTL}$ und alle $Q \in \{E, A\}$ gilt:

- a) $Q(\varphi U\psi) \equiv \psi \vee (\varphi \wedge QXQ(\varphi U\psi))$,
- b) $Q(\varphi R\psi) \equiv \psi \wedge (\varphi \vee QXQ(\varphi R\psi))$.

Beweis Betrachte den Fall $Q = E$. Die Fälle $Q = A$ werden analog bewiesen. Sei \mathcal{T} ein Transitionssystem mit Zuständen s, t, s_0, s_1, \dots , dann gilt:

(a) $\mathcal{T}, s \models E(\varphi U\psi)$ gdw. es einen Lauf s_0, s_1, \dots gibt mit $s = s_0$, und ein $k \in \mathbb{N}$, so dass $\mathcal{T}, s_k \models \psi$ und für alle $i < k$: $\mathcal{T}, s_i \models \varphi$. Betrachte zwei Fälle: Erstens, sei $k = 0$, dann gilt $\mathcal{T}, s \models \psi$ und somit auch $\mathcal{T}, s \models \psi \vee (\varphi \wedge EXE(\varphi U\psi))$.

Zweitens, sei $k > 0$. Dann gilt $\mathcal{T}, s \models \varphi$ und es gibt den Lauf s_1, s_2, \dots , welcher bezeugt, dass $\mathcal{T}, s_1 \models E(\varphi U\psi)$ gilt. Somit gilt aber auch $\mathcal{T}, s_0 \models \varphi \wedge EXE(\varphi U\psi)$, da $s_0 \rightarrow s_1$. Somit gilt auch in diesem Fall $\mathcal{T}, s \models \psi \vee (\varphi \wedge EXE(\varphi U\psi))$.

Die Rückrichtung wird genauso durch Fallunterscheidung darüber, welches Disjunkt erfüllt ist, bewiesen.

(b) Sei $\bar{E} = A$ und $\bar{A} = E$. Beachte, dass \equiv eine Kongruenzrelation ist. Somit gilt $Q(\varphi R\psi) \equiv$ (nach Lemma 3.1) $\neg\bar{Q}(\neg\varphi U\neg\psi) \equiv$ (nach Teil (a)) $\neg(\neg\psi \vee (\neg\varphi \wedge \bar{Q}X\bar{Q}(\neg\varphi U\neg\psi))) \equiv$ (nach deMorgan) $\psi \wedge (\varphi \vee \bar{Q}X\bar{Q}(\neg\varphi U\neg\psi)) \equiv$ (nach Lemma 3.1) $\psi \wedge (\varphi \vee QXQ(\neg\varphi U\neg\psi)) \equiv$ (nach Lemma 3.1) $\psi \wedge (\varphi \vee QXQ(\varphi R\psi))$. ■

Sei α eine Variable, die für CTL-Formeln steht, und $\varphi(\alpha)$ eine CTL-Formel, in der α als echte, syntaktische Unterformel auftritt. Die Semantik eines solchen φ bzgl. eines festen Transitionssystems $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ ist keine Menge von Zuständen, sondern eine Abbildung von Mengen von Zuständen auf Mengen von Zuständen. Wir notieren dies auch als $\llbracket\varphi(\alpha)\rrbracket_{[\alpha \rightarrow T]}^{\mathcal{T}}$, mit der Bedeutung, dass $\mathcal{T}, s \models \alpha$ gdw. $s \in T$. Beachte, dass $\llbracket\varphi(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi\rrbracket^{\mathcal{T}}]}^{\mathcal{T}} = \llbracket\varphi(\psi)\rrbracket^{\mathcal{T}}$ gilt.

Lemma 3.3 besagt dann nichts anderes, als dass $\llbracket Q(\varphi U\psi)\rrbracket^{\mathcal{T}}$ ein Fixpunkt der Abbildung $T \mapsto \llbracket \psi \vee (\varphi \wedge QX\alpha)\rrbracket_{[\alpha \rightarrow T]}^{\mathcal{T}}$, und $\llbracket Q(\varphi R\psi)\rrbracket^{\mathcal{T}}$ ein Fixpunkt der Abbildung $T \mapsto \llbracket \psi \wedge (\varphi \vee QX\alpha)\rrbracket_{[\alpha \rightarrow T]}^{\mathcal{T}}$ ist.

Lemma 3.4

Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ ein Transitionssystem, und $\varphi(\alpha), \psi, \psi' \in \text{CTL}$ in positiver Normalform. Falls $\llbracket\psi\rrbracket^{\mathcal{T}} \subseteq \llbracket\psi'\rrbracket^{\mathcal{T}}$, dann gilt auch $\llbracket\varphi(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi\rrbracket^{\mathcal{T}}]}^{\mathcal{T}} \subseteq \llbracket\varphi(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi'\rrbracket^{\mathcal{T}}]}^{\mathcal{T}}$.

Beweis Wir zeigen dies durch Induktion über den Formelaufbau. Die Aussage ist trivial für die atomaren Fälle $\varphi(\alpha) = q$, $\varphi(\alpha) = \neg q$ und $\varphi(\alpha) = \alpha$. Die Fälle $\varphi(\alpha) = \varphi_1(\alpha) \vee \varphi_2(\alpha)$ und $\varphi(\alpha) = \varphi_1(\alpha) \wedge \varphi_2(\alpha)$ folgen sofort aus der Induktionshypothese wegen Monotonie der mengentheoretischen Operatoren \cup und \cap .

Sei nun $\varphi(\alpha) = EX\varphi'(\alpha)$. Dann gilt

$$\begin{aligned} \llbracket\varphi(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi\rrbracket^{\mathcal{T}}]}^{\mathcal{T}} &= \{s \mid \exists t \in \mathcal{S}, s \rightarrow t \text{ und } t \in \llbracket\varphi'(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi\rrbracket^{\mathcal{T}}]}^{\mathcal{T}}\} \\ &\subseteq \{s \mid \exists t \in \mathcal{S}, s \rightarrow t \text{ und } t \in \llbracket\varphi'(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi'\rrbracket^{\mathcal{T}}]}^{\mathcal{T}}\} = \llbracket\varphi(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi'\rrbracket^{\mathcal{T}}]}^{\mathcal{T}} \end{aligned}$$

Der Fall $\varphi(\psi) = AX\varphi'(\psi)$ wird analog bewiesen.

Sei nun $\varphi(\psi) = E(\varphi_1(\alpha)U\varphi_2(\alpha))$. Dann gilt

$$\begin{aligned} &\llbracket\varphi(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi\rrbracket^{\mathcal{T}}]}^{\mathcal{T}} \\ &= \{s_0 \mid \exists \text{ Lauf } s_0, s_1, \dots, \exists k, s_k \in \llbracket\varphi_2(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi\rrbracket^{\mathcal{T}}]}^{\mathcal{T}} \text{ und } \forall i < k : s_i \in \llbracket\varphi_1(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi\rrbracket^{\mathcal{T}}]}^{\mathcal{T}}\} \\ &\subseteq \{s_0 \mid \exists \text{ Lauf } s_0, s_1, \dots, \exists k, s_k \in \llbracket\varphi_2(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi'\rrbracket^{\mathcal{T}}]}^{\mathcal{T}} \text{ und } \forall i < k : s_i \in \llbracket\varphi_1(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi\rrbracket^{\mathcal{T}}]}^{\mathcal{T}}\} \\ &\subseteq \{s_0 \mid \exists \text{ Lauf } s_0, s_1, \dots, \exists k, s_k \in \llbracket\varphi_2(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi'\rrbracket^{\mathcal{T}}]}^{\mathcal{T}} \text{ und } \forall i < k : s_i \in \llbracket\varphi_1(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi'\rrbracket^{\mathcal{T}}]}^{\mathcal{T}}\} \\ &= \llbracket\varphi(\alpha)\rrbracket_{[\alpha \rightarrow \llbracket\psi'\rrbracket^{\mathcal{T}}]}^{\mathcal{T}} \end{aligned}$$

Der Fall $\varphi(\alpha) = A(\varphi_1(\alpha)U\varphi_2(\alpha))$ wird wiederum analog bewiesen. Die verbleibenden Fälle $\varphi(\alpha) = Q(\varphi_1(\alpha)R\varphi_2(\alpha))$ folgen dann aus diesen mithilfe von Lemma 3.1. ■

3 Die Logik CTL

Man kann Lemma 3.3 nun iterativ anwenden und erhält z.B.

$$\begin{aligned}
\mathbf{E}(\varphi\mathbf{U}\psi) &\equiv \psi \vee (\varphi \wedge \mathbf{EXE}(\varphi\mathbf{U}\psi)) \\
&\equiv \psi \vee (\varphi \wedge \mathbf{EXE}(\psi \vee (\varphi \wedge \mathbf{EXE}(\varphi\mathbf{U}\psi)))) \\
&\equiv \psi \vee (\varphi \wedge \mathbf{EXE}(\psi \vee (\varphi \wedge \mathbf{EXE}(\psi \vee (\varphi \wedge \mathbf{EXE}(\varphi\mathbf{U}\psi))))) \\
&\equiv \dots
\end{aligned}$$

Es stellt sich die Frage danach, was im Limit passiert.

Definition 3.5

Seien $\varphi, \psi \in \text{CTL}$, $Q \in \{\mathbf{E}, \mathbf{A}\}$. Definiere für alle $k \in \mathbb{N}$ sogenannte *Approximanden* wie folgt.

$$\begin{aligned}
Q(\varphi\mathbf{U}^0\psi) &:= \mathbf{ff} \\
Q(\varphi\mathbf{U}^{k+1}\psi) &:= \psi \vee (\varphi \wedge Q\mathbf{X}Q(\varphi\mathbf{U}^k\psi)) \\
Q(\varphi\mathbf{R}^0\psi) &:= \mathbf{tt} \\
Q(\varphi\mathbf{R}^{k+1}\psi) &:= \psi \wedge (\varphi \vee Q\mathbf{X}Q(\varphi\mathbf{R}^k\psi))
\end{aligned}$$

Lemma 3.5

Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ ein Transitionssystem, $\varphi, \psi \in \text{CTL}$, $Q \in \{\mathbf{E}, \mathbf{A}\}$. Dann gilt für alle $k \in \mathbb{N}$:

- a) $\llbracket Q(\varphi\mathbf{U}^k\psi) \rrbracket^{\mathcal{T}} \subseteq \llbracket Q(\varphi\mathbf{U}^{k+1}\psi) \rrbracket^{\mathcal{T}}$,
- b) $\llbracket Q(\varphi\mathbf{R}^k\psi) \rrbracket^{\mathcal{T}} \supseteq \llbracket Q(\varphi\mathbf{R}^{k+1}\psi) \rrbracket^{\mathcal{T}}$,
- c) $\llbracket Q(\varphi\mathbf{U}^k\psi) \rrbracket^{\mathcal{T}} \subseteq \llbracket Q(\varphi\mathbf{U}\psi) \rrbracket^{\mathcal{T}}$,
- d) $\llbracket Q(\varphi\mathbf{R}^k\psi) \rrbracket^{\mathcal{T}} \supseteq \llbracket Q(\varphi\mathbf{U}\psi) \rrbracket^{\mathcal{T}}$.

Beweis (a) Wir zeigen die Aussage durch Induktion über k . Der Fall $k = 0$ ist trivial, da $\llbracket Q(\varphi\mathbf{U}^0\psi) \rrbracket^{\mathcal{T}} = \emptyset$. Sei nun $k > 0$. Die Induktionshypothese liefert

$$\llbracket Q(\varphi\mathbf{U}^{k-1}\psi) \rrbracket^{\mathcal{T}} \subseteq \llbracket Q(\varphi\mathbf{U}^k\psi) \rrbracket^{\mathcal{T}}$$

Laut Lemma 3.4 ist die Semantik der Formel $\psi \vee (\varphi \wedge Q\mathbf{X}Q\alpha)$ monoton in α . Also gilt

$$\llbracket Q(\varphi\mathbf{U}^k\psi) \rrbracket^{\mathcal{T}} = \llbracket \psi \vee (\varphi \wedge Q(\varphi\mathbf{U}^{k-1}\psi)) \rrbracket^{\mathcal{T}} \subseteq \llbracket \psi \vee (\varphi \wedge Q(\varphi\mathbf{U}^k\psi)) \rrbracket^{\mathcal{T}} = \llbracket Q(\varphi\mathbf{U}^{k+1}\psi) \rrbracket^{\mathcal{T}}$$

(b) Wird entweder genauso durch Induktion über k bewiesen oder folgt wiederum aus Teil (a) und Lemma 3.1.

(c) Auch dies zeigen wir durch Induktion über k . Der Induktionsanfang mit $k = 0$ ist wiederum trivial. Sei nun $k > 0$ und es gelte $\llbracket Q(\varphi\mathbf{U}^{k-1}\psi) \rrbracket^{\mathcal{T}} \subseteq \llbracket Q(\varphi\mathbf{U}\psi) \rrbracket^{\mathcal{T}}$. Dann gilt auch

$$\begin{aligned}
\llbracket Q(\varphi\mathbf{U}^k\psi) \rrbracket^{\mathcal{T}} &= \llbracket \psi \vee (\varphi \wedge Q\mathbf{X}Q(\varphi\mathbf{U}^{k-1}\psi)) \rrbracket^{\mathcal{T}} \\
&\subseteq \llbracket \psi \vee (\varphi \wedge Q\mathbf{X}Q(\varphi\mathbf{U}\psi)) \rrbracket^{\mathcal{T}} = \llbracket Q(\varphi\mathbf{U}\psi) \rrbracket^{\mathcal{T}}
\end{aligned}$$

laut Lemmas 3.4 und 3.3.

(d) Wird entweder genauso durch Induktion über k bewiesen oder folgt wiederum aus Teil (c) und Lemma 3.1. ■

Lemma 3.6

Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ ein Transitionssystem mit $|\mathcal{S}| < \infty$. Dann gilt für alle $\varphi, \psi \in \text{CTL}$, alle $s \in \mathcal{S}$ und alle $Q \in \{\mathbf{E}, \mathbf{A}\}$:

- a) $\mathcal{T}, s \models Q(\varphi\mathbf{U}\psi)$ gdw. es ein $k \in \mathbb{N}$ gibt mit $\mathcal{T}, s \models Q(\varphi\mathbf{U}^k\psi)$,
- b) $\mathcal{T}, s \models Q(\varphi\mathbf{R}\psi)$ gdw. für alle $k \in \mathbb{N}$ gilt: $\mathcal{T}, s \models Q(\varphi\mathbf{R}^k\psi)$.

Beweis (a) (\Leftarrow) Folgt sofort aus den Teilen (a) und (c) von Lemma 3.5, denn

$$\begin{aligned} & \forall s \in \mathcal{S} : ((\exists k \in \mathbb{N}, \mathcal{T}, s \models Q(\varphi\mathbf{U}^k\psi)) \Rightarrow \mathcal{T}, s \models Q(\varphi\mathbf{U}\psi)) \\ \text{gdw. } & \forall s \in \mathcal{S} : \forall k \in \mathbb{N} : (\mathcal{T}, s \models Q(\varphi\mathbf{U}^k\psi) \Rightarrow \mathcal{T}, s \models Q(\varphi\mathbf{U}\psi)) \\ \text{gdw. } & \forall k \in \mathbb{N} : \forall s \in \mathcal{S} : (\mathcal{T}, s \models Q(\varphi\mathbf{U}^k\psi) \Rightarrow \mathcal{T}, s \models Q(\varphi\mathbf{U}\psi)) \\ \text{gdw. } & \forall k \in \mathbb{N} : \llbracket Q(\varphi\mathbf{U}^k\psi) \rrbracket^{\mathcal{T}} \subseteq \llbracket Q(\varphi\mathbf{U}\psi) \rrbracket^{\mathcal{T}} \end{aligned}$$

(\Rightarrow) Laut Lemma 3.5 gilt

$$\llbracket Q(\varphi\mathbf{U}^0\psi) \rrbracket^{\mathcal{T}} \subseteq \llbracket Q(\varphi\mathbf{U}^1\psi) \rrbracket^{\mathcal{T}} \subseteq \dots \subseteq \llbracket Q(\varphi\mathbf{U}\psi) \rrbracket^{\mathcal{T}}$$

Angenommen, es gäbe ein $k \in \mathbb{N}$, so dass $\llbracket Q(\varphi\mathbf{U}^k\psi) \rrbracket^{\mathcal{T}} = \llbracket Q(\varphi\mathbf{U}^{k+1}\psi) \rrbracket^{\mathcal{T}}$. Offensichtlich gilt dann

$$\llbracket Q(\varphi\mathbf{U}^k\psi) \rrbracket^{\mathcal{T}} = \llbracket \psi \rrbracket^{\mathcal{T}} \cup (\llbracket \varphi \rrbracket^{\mathcal{T}} \cap \llbracket Q\mathbf{X}\alpha \rrbracket_{[\alpha \mapsto \llbracket Q(\varphi\mathbf{U}^k\psi) \rrbracket^{\mathcal{T}}]}^{\mathcal{T}})$$

Wir zeigen, dass in solch einem Fall gilt: $\llbracket Q(\varphi\mathbf{U}\psi) \rrbracket^{\mathcal{T}} \subseteq \llbracket Q(\varphi\mathbf{U}^k\psi) \rrbracket^{\mathcal{T}}$, was insgesamt zu zeigen ist.

Sei also $s \in \llbracket Q(\varphi\mathbf{U}\psi) \rrbracket^{\mathcal{T}}$. Die Fälle $Q = \mathbf{E}$ und $Q = \mathbf{A}$ werden separat behandelt, wobei wir uns auf $Q = \mathbf{A}$ konzentrieren, denn dieser Fall ist ungleich schwieriger. Laut Satz 3.2 gilt: $\mathcal{R}_{\mathcal{T}}(s), s \models \mathbf{A}(\varphi\mathbf{U}\psi)$. D.h. für alle Läufe $\pi = s_0, s_1, \dots$ mit $s_0 = s$ in $\mathcal{R}_{\mathcal{T}}(s)$ gibt es ein n , so dass $s_n \models \psi$ und für alle $i < n$ gilt $s_i \models \varphi$. Sei n_{π} jeweils das kleinste n mit dieser Eigenschaft bzgl. π .

Da $|\mathcal{S}| < \infty$, gelten:

1. $\mathcal{R}_{\mathcal{T}}(s)$ ist nur endlich verzweigt.
2. Auf jedem Lauf in $\mathcal{R}_{\mathcal{T}}(s)$ gibt es ab der Tiefe $|\mathcal{S}| + 1$ nur noch Zustände, die bisimilar zu einem Zustand auf demselben Lauf weiter oben sind, und somit genau dieselben CTL-Formeln erfüllen.

3 Die Logik CTL

Somit gibt es ein maximales $n_s \in \mathbb{N}$, so dass für alle Läufe π , die in s beginnen, gilt: $n_\pi \leq n_s$. Wir fahren fort mit Induktion nach n_s .

Fall $n_s = 0$. Somit gilt $s_0 \models \psi$ für jeden Lauf s_0, s_1, \dots mit $s_0 = s$, also $s \in \llbracket \psi \rrbracket^{\mathcal{R}_{\mathcal{T}}(s)}$ und dann auch $s \in \llbracket Q(\varphi \mathbf{U}^k \psi) \rrbracket^{\mathcal{T}}$.

Fall $n_s > 0$. D.h. es gibt mindestens einen Lauf $\pi = s_0, s_1, \dots$ mit $n_\pi > 0$, also $s_0 \models \varphi$ und somit $s \in \llbracket \varphi \rrbracket^{\mathcal{R}_{\mathcal{T}}(s)}$. Außerdem gilt $s \not\models \psi$, denn ansonsten wäre $n_s = 0$. Dann muss aber für alle t mit $s \rightarrow t$ gelten: $\mathcal{R}_{\mathcal{T}}(s), t \models \mathbf{A}(\varphi \mathbf{U} \psi)$. Da alle Läufe, die in t anfangen, echte Suffixe eines Laufes sind, der in s anfängt, gilt $n_t < n_s$, und die Induktionshypothese liefert: $t \in \llbracket \mathbf{A}(\varphi \mathbf{U}^k \psi) \rrbracket^{\mathcal{R}_{\mathcal{T}}(s)}$ für alle t mit $s \rightarrow t$. Somit gilt auch $s \in \llbracket \mathbf{AXA}(\varphi \mathbf{U}^k \psi) \rrbracket^{\mathcal{R}_{\mathcal{T}}(s)}$ und dann auch $s \in \llbracket \mathbf{A}(\varphi \mathbf{U}^k \psi) \rrbracket^{\mathcal{R}_{\mathcal{T}}(s)}$. Laut Satz 3.2 folgt auch dann $s \in \llbracket \mathbf{A}(\varphi \mathbf{U}^k \psi) \rrbracket^{\mathcal{T}}$.

Somit gilt insgesamt $\llbracket \mathbf{A}(\varphi \mathbf{U} \psi) \rrbracket^{\mathcal{T}} \subseteq \llbracket \mathbf{A}(\varphi \mathbf{U}^k \psi) \rrbracket^{\mathcal{T}}$.

Es bleibt noch zu zeigen, dass es immer ein solches k geben muss. Dies folgt aber sofort aus $|\llbracket Q(\varphi \mathbf{U} \psi) \rrbracket^{\mathcal{T}}| \leq |\mathcal{S}| < \infty$, womit die obige Kette der Approximanden bei einem k stationär werden muss.

(b) Es gilt

$$\begin{aligned} \mathcal{T}, s \models Q(\varphi \mathbf{R} \psi) & \text{ gdw. } \mathcal{T}, s \not\models \overline{Q}(\neg \varphi \mathbf{U} \neg \psi) \\ & \text{ gdw. } \nexists k \in \mathbb{N} : \mathcal{T}, s \models \overline{Q}(\neg \varphi \mathbf{U}^k \neg \psi) \\ & \text{ gdw. } \forall k \in \mathbb{N} : \mathcal{T}, s \not\models \overline{Q}(\neg \varphi \mathbf{U}^k \neg \psi) \\ & \text{ gdw. } \forall k \in \mathbb{N} : \mathcal{T}, s \models Q(\varphi \mathbf{R}^k \psi) \end{aligned}$$

laut Teil (a) und Lemma 3.1. Durch Induktion über k zeigt man außerdem leicht, dass für alle $k \in \mathbb{N}$ gilt: $Q(\varphi \mathbf{U}^k \psi) \equiv \neg \overline{Q}(\neg \varphi \mathbf{R}^k \neg \psi)$. ■

3.3.2 Das Model Checking Problem

Mithilfe von Lemma 3.6 läßt sich nun ein globaler Model Checking Algorithmus für CTL auf endlichen, totalen, knotenbeschrifteten Transitionssystemen angeben.

Satz 3.3

Das Model Checking Problem für CTL ist in P.

Beweis Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ mit $|\mathcal{S}| < \infty$. Der in Abb. 3.1 dargestellte, deterministische Algorithmus MC-CTL nimmt eine CTL-Formel φ und berechnet die Menge aller Zustände $s \in \mathcal{S}$, für die $s \models \varphi$ gilt. Wegen Lemma 3.1 beschränken wir uns auf Formeln, die aus atomaren Propositionen mittels Disjunktionen, Negationen und den temporalen Operatoren EX, EU und ER aufgebaut sind.

Es bleibt zu zeigen, dass MC-CTL auf φ in Polynomialzeit terminiert und genau $\llbracket \varphi \rrbracket^{\mathcal{T}}$ zurückliefert.

```

Algorithmus MC-CTL( $\varphi$ )
  case  $\varphi$  of
     $q$       : return  $\{s \mid q \in \lambda(s)\}$ 
     $\psi_1 \vee \psi_2$  : return  $\text{MC-CTL}(\psi_1) \cup \text{MC-CTL}(\psi_2)$ 
     $\neg\psi$     : return  $\mathcal{S} \setminus \text{MC-CTL}(\psi)$ 
     $\text{EX}\psi$    :  $T := \text{MC-CTL}(\psi)$ 
               return  $\{s \mid \exists t \in T, s \rightarrow t\}$ 
     $\text{E}(\psi_1 \text{U} \psi_2)$  :  $P_1 := \text{MC-CTL}(\psi_1)$ 
                        $P_2 := \text{MC-CTL}(\psi_2)$ 
                        $S := \emptyset$ 
                       repeat
                          $T := S$ 
                          $T' := \{s \mid \exists t \in T, s \rightarrow t\}$ 
                          $S := P_2 \cup (P_1 \cap T')$ 
                       until  $T = S$ 
                       return  $S$ 
     $\text{E}(\psi_1 \text{R} \psi_2)$  :  $P_1 := \text{MC-CTL}(\psi_1)$ 
                        $P_2 := \text{MC-CTL}(\psi_2)$ 
                        $S := \mathcal{S}$ 
                       repeat
                          $T := S$ 
                          $T' := \{s \mid \exists t \in T, s \rightarrow t\}$ 
                          $S := P_2 \cap (P_1 \cup T')$ 
                       until  $T = S$ 
                       return  $S$ 
    
```

Abbildung 3.1: Ein globaler Model Checking Algorithmus für CTL.

Termination. Wir zeigen durch Induktion über den Aufbau von φ , dass MC-CTL auf $\varphi \in \text{CTL}$ in Zeit $O(|\rightarrow| \cdot |\varphi|)$ terminiert. Dies ist offensichtlich der Fall für atomare Propositionen und folgt sofort per Hypothese für Negationen. Für Disjunktionen ist dies nicht offensichtlich, denn es gilt nicht unbedingt $\varphi = \psi_1 \vee \psi_2$ impliziert $|\varphi| \geq |\psi_1| + |\psi_2| + 1$, da ψ_1 und ψ_2 gemeinsame Unterformeln haben können. Läßt man MC-CTL jedoch in einer Tabelle bereits Ergebnisse abspeichern und vor jedem Aufruf abfragen, ob der Wert zu dem aktuellen Argument bereits berechnet wurde, dann ist auch die Laufzeit im Falle einer Disjunktion durch $O(|\rightarrow| \cdot |\varphi|)$ beschränkt.

Sei $\varphi = \text{EX}\psi$. Laut Hypothese terminiert der rekursive Aufruf in $O(|\rightarrow| \cdot |\psi|)$ vielen Schritten. In weiteren $|\rightarrow|$ vielen Schritten lassen sich alle Zustände bestimmen, die einen Nachfolger in einer gegebenen Menge haben. Somit ist die Behauptung auch für diesen Fall bewiesen.

Sei $\varphi = \text{E}(\psi_1 \text{U} \psi_2)$. Beachte, dass die **repeat/until**-Schleife in diesem Fall die Iteration

3 Die Logik CTL

einer monotonen Abbildung, beginnend mit \emptyset , realisiert. Somit tritt der Abbruchfall nach spätestens $|\mathcal{S}|$ vielen Iterationen ein. Da \mathcal{T} total ist, gilt $|\mathcal{S}| \leq |\rightarrow|$. Für die rekursiven Aufrufe vorher gilt dieselbe Überlegung wie im Fall einer Disjunktion. Der Fall $\varphi = \mathbf{E}(\psi_1 \mathbf{R} \psi_2)$ wird genauso behandelt.

Korrektheit. Wir zeigen, wieder durch Induktion über den Aufbau von φ , dass gilt: $\text{MC-CTL}(\varphi) = T$ gdw. $T = \llbracket \varphi \rrbracket^{\mathcal{T}}$. Der atomare Fall ist wiederum trivial, und die Fälle einer Disjunktion, Negation oder des EX-Operators folgen sofort aus der Induktionshypothese.

Für den Fall $\varphi = \mathbf{E}(\psi_1 \mathbf{U} \psi_2)$ beachte, dass die **repeat/until**-Schleife in der Variablen S sukzessive die Approximanden $\mathbf{E}(\psi_1 \mathbf{U}^0 \psi_2)$, $\mathbf{E}(\psi_1 \mathbf{U}^1 \psi_2)$, ... berechnet. Korrektheit in diesem Fall folgt somit aus Lemma 3.6. Der Fall $\varphi = \mathbf{E}(\psi_1 \mathbf{R} \psi_2)$ wird wiederum genauso behandelt. ■

Zusammen mit Korollar 3.1 ergibt sich Vollständigkeit.

Korollar 3.2

Das Model Checking Problem für CTL ist P-vollständig.

Algorithmus MC-CTL ist *global* in dem Sinne, dass er zu einer gegebenen Formel φ alle Zustände eines gegebenen Transitionssystems berechnet, die φ erfüllen. In der Programmverifikation interessiert man sich oft jedoch lediglich für die Frage, ob ein gegebener Zustand eines Transitionssystems eine gegebene Formel erfüllt. Dies zu lösen kann u.U. mit wesentlich weniger Aufwand verbunden sein, wenn man – von der Formel geleitet – versucht, einen Grund dafür, dass der gegebene Zustand die Formel (nicht) erfüllt, in dem Transitionssystem zu finden. Da dies bereits von der Problembeschreibung her einem logischen Beweisverfahren ähnelt, benutzen wir tableau-ähnliche Verfahren zum *lokalen Model Checking*.

Ein *Tableau* ist dabei lediglich ein beschrifteter Baum, der gemäss einer Menge von Regeln aus einem Wurzelknoten konstruiert wird. Bäume wachsen hier nach oben, und die Regeln sind so zu lesen, dass man, um die untere Aussage zu beweisen, alle oberen Aussagen beweisen muss. Erstere nennt man auch *Konklusion*, letztere heißen *Prämisen*.

Definition 3.6

Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda, s_0)$ ein totales, knoten-beschriftetes und endliches Transitionssystem. Ein *Model Checking Tableau* für eine CTL-Formel φ in positiver Normalform und den Zustand s_0 ist ein Baum, dessen Knoten mit Paaren aus $\mathcal{S} \times \text{Sub}^*(\varphi)$ beschriftet sind. Ein solcher, möglicherweise unendlicher Baum heißt *Prä-Tableau*, wenn gilt:

- Die Wurzel ist mit $s_0 \vdash \varphi_0$ beschriftet.
- Die Beschriftung eines Knoten, der kein Blatt ist, bildet mit den Beschriftungen seiner direkten Nachfolger eine Instanz einer der folgenden Regeln.

$$(\wedge) \frac{s \vdash \varphi_1 \quad s \vdash \varphi_2}{s \vdash \varphi_1 \wedge \varphi_2} \quad (LV) \frac{s \vdash \varphi_1}{s \vdash \varphi_1 \vee \varphi_2} \quad (RV) \frac{s \vdash \varphi_2}{s \vdash \varphi_1 \vee \varphi_2}$$

$$\begin{array}{c}
 (\text{EX}) \frac{t \vdash \varphi}{s \vdash \text{EX}\varphi} \quad s \rightarrow t \quad (\text{AX}) \frac{t_1 \vdash \varphi \dots t_n \vdash \varphi}{s \vdash \text{AX}\varphi} \quad \{t_1, \dots, t_n\} = \{t \mid s \rightarrow t\} \\
 \\
 (\text{QU}) \frac{s \vdash \psi \vee (\varphi \wedge \text{QXQ}(\varphi\text{U}\psi))}{s \vdash \text{Q}(\varphi\text{U}\psi)} \quad (\text{QR}) \frac{s \vdash \psi \wedge (\varphi \vee \text{QXQ}(\varphi\text{R}\psi))}{s \vdash \text{Q}(\varphi\text{R}\psi)}
 \end{array}$$

Ein endliches Prä-Tableau heißt *Tableau*, wenn jedes Blatt eine der folgenden Bedingungen erfüllt. Die Beschriftung ist entweder von der Form

- $s \vdash q$, so dass $q \in \lambda(s)$ gilt, oder
- $s \vdash \neg q$, so dass $q \notin \lambda(s)$ gilt, oder
- $s \vdash \text{Q}(\varphi\text{R}\psi)$, so dass es auf demselben Pfad einen weiteren Knoten mit derselben Beschriftung gibt.

Wir schreiben auch einfach $s \vdash \varphi$, wenn es ein Tableau mit Wurzel $s \vdash \varphi$ gibt.

Wir nennen einen Knoten $s \vdash \varphi$ eines (Prä-)Tableaus *wahr*, wenn $s \models \varphi$ gilt und falsch sonst.

Beispiel 3.3

Sei $\mathcal{T} = (\{s, t\}, \rightarrow, \lambda, s)$ mit $s \rightarrow s$, $s \rightarrow t$, $t \rightarrow t$ und $\lambda(s) = \emptyset$, $\lambda(t) = \{q\}$. Betrachte die CTL-Formel $\varphi := \text{AGEF}q$. Es gilt $\mathcal{T}, s \models \varphi$, denn sowohl s als auch t erfüllen die Formel $\text{EF}q$ wegen den Läufen s, t, t, \dots bzw. t, t, \dots . Der folgende Baum ist ein Prä-Tableau für \mathcal{T} , s und φ .

$$\begin{array}{c}
 \frac{t \vdash q}{t \vdash q \vee \text{EXEF}q} \quad \frac{t \vdash q}{t \vdash q \vee \text{EXEF}q} \quad \frac{t \vdash \text{AGEF}q}{t \vdash \text{AGEF}q} \\
 \frac{t \vdash \text{EF}q}{s \vdash \text{EXEF}q} \quad \frac{t \vdash \text{EF}q \quad t \vdash \text{AXAGEF}q}{t \vdash \text{EF}q \wedge \text{AXAGEF}q} \\
 \frac{s \vdash q \vee \text{EXEF}q}{s \vdash \text{EF}q} \quad \frac{s \vdash \text{AGEF}q}{s \vdash \text{AXAGEF}q} \quad \frac{t \vdash \text{AGEF}q}{t \vdash \text{AGEF}q} \\
 \frac{s \vdash \text{EF}q \quad s \vdash \text{AXAGEF}q}{s \vdash \text{EF}q \wedge \text{AXAGEF}q} \\
 \frac{s \vdash \text{EF}q \wedge \text{AXAGEF}q}{s \vdash \text{AGEF}q}
 \end{array}$$

Offensichtlich ist dieses Prä-Tableau auch ein Tableau, denn der (von links nach rechts) erste und dritte Pfad erfüllen die erste, der zweite und vierte jeweils die dritte Bedingung an Pfade eines Tableaus. Beachte, dass EG ein Spezialfall von ER ist.

Satz 3.4

Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda, s_0)$ ein endliches Transitionssystem und $\varphi \in \text{CTL}$. Wenn $s_0 \models \varphi_0$, dann $s_0 \vdash \varphi_0$.

3 Die Logik CTL

Beweis Angenommen, $s \models \varphi$. Es ist leicht zu sehen, dass sich zu jedem Paar aus Zustand und Formel in positiver Normalform immer ein Prä-Tableau konstruieren läßt. Dies liegt daran, dass es für jeden Formeltyp eine Regel gibt und Transitionssysteme als total angenommen werden. Außerdem läßt sich dieses Prä-Tableau so konstruieren, dass alle Knoten wahr sind. Dies sieht man leicht durch Inspektion der Regeln und der Semantik von CTL-Formeln. Für die Operatoren QU und QR folgt dies aus Lemma 3.3. Es bleibt zu zeigen, dass dieses Prä-Tableau ein Tableau ist.

Angenommen, dem sein nicht so. Dann gibt es zwei Fälle. Erstens, es gibt ein Blatt $s \vdash q$ mit $q \notin \lambda(s)$ oder $s \vdash \neg q$ mit $q \in \lambda(s)$. Solche Knoten sind jedoch nicht wahr, was der Annahme widerspricht, dass alle Knoten in diesem Prä-Tableau wahr sind.

Zweitens, es gibt einen unendlichen Pfad. Da aber $|\mathcal{S} \times \text{Sub}^*(\varphi)| < \infty$ gilt, gibt es auf diesem Pfad zwei Knoten mit derselben Beschriftung. Da alle Regeln außer denen für die Operatoren QU und QR die Größe einer Beschriftung echt verringern, muss es auch auf diesem Pfad zwei Knoten v und v' mit derselben Beschriftung von der Form $s \vdash Q(\varphi U \psi)$ oder $s \vdash Q(\varphi R \psi)$ geben. O.B.d.A. komme v' nach v auf diesem Pfad vor. Im Fall QR trifft jedoch auf v' eine Tableau-Bedingung an ein Blatt zu. Nehmen wir also an, dass der QU -Fall zutrifft.

Seien v_1, \dots, v_n alle Knoten auf dem Pfad von v nach v' der Form $t \vdash Q(\varphi U \psi)$. Beachte, dass diese Formel immer mit Regel (U) zu einer Disjunktion abgewickelt wird, und danach immer Regel ($R\vee$) gewählt wurde. Ansonsten wäre $Q(\varphi U \psi)$ eine echte Unterformel von ψ .

Angenommen, jedes solche v_i sei mit $s_i \vdash Q(\varphi U \psi)$ beschriftet. Nach Lemma 3.6 existiert für jedes $i \in \{1, \dots, n\}$ ein kleinstes k_i , so dass $s_i \models Q(\varphi U^{k_i} \psi)$. Da die Regeln der Struktur der Approximanden aus Def. 3.5 folgen und zwischen v_i und v_{i+1} immer Regel (QU) angewandt wird, gilt $k_1 > k_2 > \dots > k_n$. Da $s_1 = s_n$ müsste aber $k_1 = k_n$ gelten.

Wir schließen, dass alle Pfade in diesem Prä-Tableau irgendwann eine der Abbruchbedingungen erfüllen müssen, und somit das Prä-Tableau ein Tableau ist. Also gilt $s_0 \vdash \varphi_0$. ■

Satz 3.5

Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda, s_0)$ ein endliches Transitionssystem und $\varphi \in \text{CTL}$. Wenn $s_0 \vdash \varphi_0$, dann $s_0 \models \varphi_0$.

Beweis Angenommen $s_0 \not\models \varphi_0$, aber es gibt ein Tableau für $s_0 \vdash \varphi_0$, dessen Wurzel nicht wahr ist. Beachte, dass alle Regeln folgende Eigenschaft erfüllen: Wenn die Konklusion nicht wahr ist, dann gibt es eine Prämisse, die nicht wahr ist. Somit muss es in diesem Tableau einen Pfad geben, auf dem alle Knoten nicht wahr sind.

Wiederum ist es leicht zu sehen, dass dieser Pfad nicht in einem Blatt der Form $t \vdash q$ oder $t \vdash \neg q$ enden kann, denn Blätter dieser Form sind in jedem Tableau wahr. Also muss es auf diesem Pfad einen inneren Knoten v und ein Blatt v' der Form $s \vdash Q(\varphi R \psi)$ geben. Da diese falsch sind, gibt es laut Lemma 3.6 wiederum jeweils kleinste k, k' , so dass $s \not\models Q(\varphi R^k \psi)$ und $s \not\models Q(\varphi R^{k'} \psi)$ und $k' < k$. Dies ist aber ein Widerspruch, da nicht beide gleichzeitig kleinst sein können. ■

3.3.3 Das Erfüllbarkeitsproblem

Wir kombinieren Ideen aus dem Algorithmus SAT-HML, der Erfüllbarkeit für HML-Formeln testet, und den Model Checking Tableaux aus dem vorigen Abschnitt, um Erfüllbarkeitstableaux für CTL zu erhalten. Die äquivalenzerhaltenden Fixpunktentwicklungen aus Lemma 3.3 liefern uns dabei wieder eine Methode, mit den temporalen Operatoren QU und QR umzugehen. Da die (Un-)Erfüllbarkeit einer Konjunktion nicht auf die (Un-)Erfüllbarkeit ihrer Konjunkte zurückgeführt werden kann, müssen die Knoten der Tableaux mit Mengen von Formeln beschriftet werden.

Definition 3.7

Sei φ_0 eine CTL-Formel in positiver Normalform. Ein (Erfüllbarkeits-)Prä-Tableau für φ_0 ist ein möglicherweise unendlicher Baum, dessen Knoten mit Teilmengen von $Sub^*(\varphi_0)$ beschriftet sind, so dass

- die Wurzel mit φ_0 beschriftet ist, und
- die Beschriftungen eines inneren Knoten zusammen mit den Beschriftungen seiner Nachfolger eine Instanz einer der folgenden Regeln bilden.

$$(\wedge) \frac{\psi_0, \psi_1, \Phi}{\psi_0 \wedge \psi_1, \Phi} \quad (L\vee) \frac{\psi_0, \Phi}{\psi_0 \vee \psi_1, \Phi} \quad (R\vee) \frac{\psi_1, \Phi}{\psi_0 \vee \psi_1, \Phi}$$

$$(U) \frac{\psi \vee (\varphi \wedge QXQ(\varphi U\psi)), \Phi}{Q(\varphi U\psi), \Phi} \quad (R) \frac{\psi \wedge (\varphi \vee QXQ(\varphi R\psi)), \Phi}{Q(\varphi R\psi), \Phi}$$

$$(X) \frac{\varphi_1, \psi_1, \dots, \psi_m \quad \dots \quad \varphi_n, \psi_1, \dots, \psi_m}{EX\varphi_1, \dots, EX\varphi_n, AX\psi_1, \dots, AX\psi_m, l_1, \dots, l_k} \text{ falls } l_1, \dots, l_k \text{ konsistent}$$

Eine *Hauptformel* in einer Beschriftung ist diejenige Formel, die durch Anwenden einer Regel ersetzt wird. Beachte, dass im Fall der letzten Regel alle nicht-atomaren Formeln Hauptformeln sind.

Das folgende Beispiel zeigt, dass es jedoch nicht mehr möglich ist, die Abbruchbedingung für einen Tableau-Pfad nur über die Wiederholung einer Beschriftung auf einem Pfad zu definieren.

Beispiel 3.4

Sei φ die CTL-Formel $AFq \wedge EXEGAFq$. Offensichtlich ist φ erfüllbar, z.B. in dem totalen Modell, welches nur aus einem Zustand besteht, der mit q beschriftet ist. Betrachte jedoch die folgenden beiden Prä-Tableaux.

$\frac{\frac{\frac{\text{AF}q \wedge \text{EXEGAF}q}{\text{EGAF}q}}{q, \text{EXEGAF}q}}{q \vee \text{AXAF}q, \text{EXEGAF}q}$	$\frac{\frac{\frac{\text{AF}q, \text{EXEGAF}q}{\text{AF}q, \text{AF}q \wedge \text{EXEGAF}q}}{\text{AF}q, \text{EGAF}q}}{\text{AXAF}q, \text{EXEGAF}q}}$
$\frac{\text{AF}q, \text{EXEGAF}q}{\text{AF}q \wedge \text{EXEGAF}q}$	$\frac{\text{AF}q, \text{EXEGAF}q}{\text{AF}q \wedge \text{EXEGAF}q}$

In beiden Prä-Tableaux tritt eine Wiederholung einer Beschriftung auf. Im linken ist jedoch das U aus der Formel $\text{AF}q$ durch die Wahl des linken Disjunktts erfüllt worden. Sieht man solch ein Prä-Tableau als Versuch einer Modellkonstruktion, dann ist diese im linken Fall gelungen. Im rechten Prä-Tableau ist das Erfüllen des U aufgeschoben worden, so dass in der gedachten Modellkonstruktion kein Zustand erzeugt wurde, in dem q gelten muss. Daher kann der Pfad in dem rechten Prä-Tableau auch nicht als Tableau-Pfad zählen.

Definition 3.8

Sei $\pi = \Phi_0, \Phi_1, \dots, \Phi_n$ ein endlicher Pfad in einem Prä-Tableau, d.h. für alle $i = 1, \dots, n$ gilt: Φ_i ist eine Prämisse von Φ_{i-1} . Ein *interner Pfad* in π ist eine Sequenz ψ_0, \dots, ψ_n , so dass für alle $i = 1, \dots, n$ gilt entweder

- ist ψ_i aus der Hauptformel ψ_{i-1} durch Anwenden einer Regel entstanden, oder
- $\psi_i = \psi_{i-1}$.

Ein endliches Prä-Tableau ist ein *Tableau*, wenn für jeden Pfad Φ_0, \dots, Φ_n , wobei Φ_n ein Blatt ist, eine der folgenden Bedingungen gilt:

1. $\Phi_n = l_1, \dots, l_k$ ist, so dass Φ_n eine konsistente Menge von Literalen bildet, oder
2. es gibt ein $i < n$, so dass $\Phi_i = \Phi_n$ und es gibt kein $\chi \in \Phi_n$ von der Form $Q(\varphi U \psi)$ mit einem internen Pfad von χ in Φ_i zu $\chi \in \Phi_n$.

Satz 3.6

Sei φ_0 eine CTL-Formel in positiver Normalform. Wenn φ_0 erfüllbar ist, dann existiert ein Erfüllbarkeitstableau für φ_0 .

Beweis Angenommen, φ_0 hat ein Modell $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda, s_0)$. Wegen Satz 3.2 können wir davon ausgehen, dass \mathcal{T} ein unendlicher Baum mit Wurzel s_0 ist. Wir benutzen \mathcal{T} , um ein (möglicherweise) unendliches Prä-Tableau für φ_0 zu konstruieren. Die Konstruktion bezieht sich knotenweise auf jeweils einen Zustand des Transitionssystems, so dass die folgende Invariante erhalten bleibt.

Wenn ein Knoten mit Bezug auf den Zustand s die Beschriftung Φ hat, dann gilt $s \models \bigwedge \Phi$.

Die Wurzel bezieht sich auf s_0 und ist beschriftet mit φ_0 . Lemmas 2.2 und 2.3 (in entsprechender Weise für CTL formuliert) zeigen, dass es immer möglich ist, diese Invariante in einer Regelanwendung zu erhalten. Zusätzlich verlangen wir, dass in den Fällen, in denen sowohl (LV) als auch (RV) angewendet werden können, die Regel (LV) zum Zuge kommt.

Es bleibt zu zeigen, dass aus solch einem Prä-Tableau ein Tableau gewonnen werden kann. Dazu unterscheiden wir endliche und unendliche Pfade in diesem Prä-Tableau. Offensichtlich bestehen Blätter in diesem Prä-Tableau nur aus Literalen l_1, \dots, l_k . Wegen der erhaltenen Invariante trifft die Tableau-Bedingung (1) auf endliche Pfade zu.

Sei nun Φ_0, Φ_1, \dots ein unendlicher Pfad, so dass für alle $i \in \mathbb{N}$ die Menge Φ_i jeweils in Bezug auf einen Zustand s_i konstruiert wurde. Dann ist s_0, s_1, \dots ein Lauf durch \mathcal{T} . Da $|Sub^*(\varphi_0)| < \infty$ gibt es ein $\Phi \subseteq Sub^*(\varphi_0)$ so dass $\Phi = \Phi_i$ für unendlich viele i . Da nur die Regeln (U) und (R) größere Prämissen als Konklusionen haben, muss zwischen zwei Auftreten von Φ mindestens eine dieser Regeln angewandt worden sein. Somit sind diese Auftreten nicht identisch.

Beachte außerdem, dass es keinen internen Pfad unendlicher Länge durch Φ_0, Φ_1, \dots geben kann, auf dem unendlich oft eine Formel der Form $Q(\varphi U \psi)$ vorkommt. Denn die Invariante garantiert, dass bei jedem Auftreten in Bezug auf ein s_i es ein s_j mit $j \geq i$ gibt, so dass $s_j \models \psi$. Dann würde die Prä-Tableau-Konstruktion aber an dieser Stelle die Regel (LV) statt (RV) anwenden, und ψ anstelle von $\varphi \wedge QXQ(\varphi U \psi)$ ist dann die Formel auf diesem internen Pfad. Da $Q(\varphi U \psi) \notin Sub^*(\psi)$, kommt auf diesem internen Pfad $Q(\varphi U \psi)$ auch nicht mehr vor.

Somit muss es zwei Auftreten von Φ geben, so dass es zwischen diesen keinen internen Pfad gibt, der in einem QU beginnt und endet. Wird dieser unendliche Pfad bei dem zweiten Auftreten abgeschnitten, dann erfüllt er die Bedingung (2) an Tableau-Pfade. Daher existiert dann auch ein Tableau für φ_0 . ■

Satz 3.7

Sei φ_0 eine CTL-Formel in positiver Normalform. Wenn ein Erfüllbarkeitstableau für φ_0 existiert, dann ist φ_0 erfüllbar.

Beweis Angenommen, es existiert ein Tableau T für φ_0 . Beachte, dass es für jeden Knoten v höchstens einen Knoten w gibt, der über v liegt und

- entweder ein Blatt mit literaler Beschriftung oder
- die Konklusion einer Anwendung der Regel (X) ist.

Dies liegt daran, dass nur die Regel (X) mehrere Prämissen haben kann. Für solche v , denen nicht solch ein w zugeordnet werden kann, gibt es jedoch ein eindeutiges Blatt, welches laut Tableau-Bedingung (1) identisch ist mit einem Vorgänger von v . Dazwischen muss ebenfalls irgendwann zum ersten Mal Regel (X) angewandt werden. Somit ist jedem v eindeutig solch ein w zuzuordnen, welches wir mit $f(v)$ bezeichnen. Beachte, dass der literale Teil der Beschriftung von $f(v)$ immer konsistent ist.

Definiere nun ein Transitionssystem $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ wie folgt

3 Die Logik CTL

- $\mathcal{S} = \{(v) \mid v \text{ ist Knoten in dem Tableau } T \}$,
- $f(v) \rightarrow f(w)$, falls w Prämisse von $f(v)$ ist,
- $\lambda(f(v)) = \{q \mid q \text{ ist in der Beschriftung von } f(v) \text{ enthalten}\}$.

Es bleibt zu zeigen, dass $\mathcal{T}, f(v_0) \models \varphi_0$ gilt, wobei v_0 die Wurzel von T ist. Wir zeigen die folgende, stärkere Aussage durch Induktion über den Formelaufbau. Für alle Knoten v von T mit Beschriftung Φ und alle $\varphi \in \Phi$ gilt: $f(v) \models \varphi$.

Für atomare Formeln $\varphi = q$ oder $\varphi = \neg q$ folgt dies sofort aus der Definition von λ . Der Fall $\varphi = \psi_0 \wedge \psi_1$ folgt sofort aus der Induktionshypothese, da zwischen einem v , dessen Beschriftung φ enthält und $f(v)$ ein w liegen muss, so dass $f(v) = f(w)$ und w mit ψ_0 und ψ_1 beschriftet ist. Dasselbe gilt für Disjunktionen.

Sei $\varphi = \text{EX}\psi$. Nach Induktionshypothese gilt $f(w) \models \psi$ für jeden Knoten w , der mit ψ beschriftet ist. Die Aussage folgt für diesen Fall dann sofort aus der Tatsache, dass es ein w gibt, so dass $f(v) \rightarrow f(w)$ und w mit ψ beschriftet ist. Der Fall $\varphi = \text{AX}\psi$ wird analog bewiesen.

Sei $\varphi = Q(\psi_1 \mathbf{R} \psi_2)$. Da T endlich ist, ist auch \mathcal{T} endlich, und laut Lemma 3.6 reicht es aus zu zeigen, dass $f(v) \models Q(\psi_1 \mathbf{R}^k \psi_2)$ für alle $k \in \mathbb{N}$ gilt. Dies ist offensichtlich der Fall für $k = 0$. Sei nun $k > 0$ und die Aussage bereits bewiesen für $k - 1$. Beachte, dass es für jedes v , welches mit $Q(\psi_1 \mathbf{R} \psi_2)$ beschriftet ist, ein w gibt, welches mit $\psi_2 \wedge (\psi_1 \vee Q\mathbf{X}Q(\psi_1 \mathbf{R} \psi_2))$ beschriftet ist, so dass $f(v) = f(w)$ gilt. Die Hypothese der Hauptinduktion liefert uns dann $f(v) \models \psi_2$ und entweder $f(v) \models \psi_1$, oder es gilt $f(v) \models Q\mathbf{X}Q(\psi_1 \mathbf{R}^{k-1} \psi_2)$ nach der Hypothese der Nebeninduktion. Somit gilt nach der Definition der Approximanden auch $f(v) \models Q(\psi_1 \mathbf{R}^k \psi_2)$.

Sei nun $\varphi = Q(\psi_1 \mathbf{U} \psi_2)$. Betrachte zuerst separat den Fall $Q = \mathbf{E}$. Es ist leicht zu sehen, dass es eine Sequenz v, \dots von Knoten gibt, in deren Beschriftungen ein interner Pfad, beginnend mit φ existiert, der nur zu Beginn nur aus den Formeln $Q(\psi_1 \mathbf{U} \psi_2)$, $Q\mathbf{X}Q(\psi_1 \mathbf{U} \psi_2)$, $\psi_1 \wedge Q\mathbf{X}Q(\psi_1 \mathbf{U} \psi_2)$ und $\psi_2 \vee (\psi_1 \wedge Q\mathbf{X}Q(\psi_1 \mathbf{U} \psi_2))$ besteht. Da wegen Tableau-Bedingung (1) jedoch irgendwann ein w erreicht sein muss, so dass dieser interne Pfad in w in die Formel ψ_2 mündet, gilt nach Hypothese $f(w) \models \psi$. Durch Anwenden der Hypothese für ψ_1 auf den dazwischenliegenden Knoten und der Definition von \rightarrow sieht man leicht, dass dann auch $f(v) \models \mathbf{E}(\psi_1 \mathbf{U} \psi_2)$ gilt. Der Fall $Q = \mathbf{A}$ wird wiederum analog gezeigt. ■

Korollar 3.3

Für alle $\varphi \in \text{CTL}$ gilt: Falls φ erfüllbar ist, dann hat φ ein endliches Modell.

Beweis Übung. ■

Satz 3.8 (ohne Beweis)

Das Erfüllbarkeitsproblem für CTL ist in EXPTIME.

Satz 3.9 (Übung)

Das Erfüllbarkeitsproblem für CTL ist EXPTIME-hart.

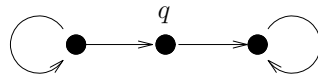
Korollar 3.10 *Das Erfüllbarkeitsproblem für CTL ist EXPTIME-vollständig.*

3.4 Ausdrucksstärke

Wie in Abschnitt 3.1 gezeigt, lässt sich in CTL ausdrücken, dass auf allen Läufen eines Transitionssystems unendlich oft ein Zustand vorkommt, der mit q beschriftet ist: $\text{AGAF}q$. Beachte, dass “unendlich oft” hier nur eine Konsequenz aus “überall immer wieder” ist. Dass dies mit dem universellen Pfadquantor A zu tun hat, wird von der Formel $\text{EGEF}q$ gezeigt. Diese drückt nicht etwa “es gibt einen Pfad, auf dem unendlich oft q gilt” aus, wie folgendes Beispiel zeigt.

Beispiel 3.5

Der linke Zustand des Transitionssystems



erfüllt die Formel $\text{EGEF}q$, denn für den Lauf, der immer im linken Zustand verbleibt, gilt an jeder Stelle: es gibt einen Lauf – nämlich den, der in den rechten Zustand führt, auf dem irgendwann einmal q gilt. Allerdings gibt es keinen Lauf, auf dem unendlich oft q gilt.

Definition 3.9

Ähnlich zur modalen Tiefe einer HML-Formel definieren wir die *temporale Tiefe* einer CTL-Formel φ als die maximale Anzahl $td(\varphi)$ von temporalen Operatoren auf einem Pfad im Syntaxbaum von φ . Wegen Lemma 3.1 beschränken wir uns hier wieder auf Formeln, die aus atomaren Propositionen mithilfe von Disjunktionen, Negationen und den temporalen Operatoren EX , EU und ER aufgebaut sind.

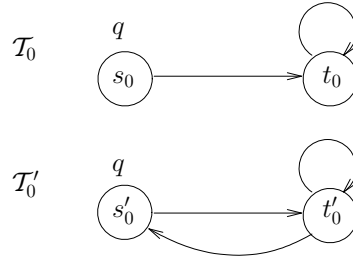
$$\begin{aligned}
 td(q) &:= 0 \\
 td(\varphi \vee \psi) &:= \max\{td(\varphi), td(\psi)\} \\
 td(\neg\varphi) &:= td(\varphi) \\
 td(\text{EX}\varphi) &:= 1 + td(\varphi) \\
 td(\text{EU}\varphi) &:= 1 + \max\{td(\varphi), td(\psi)\} \\
 td(\text{ER}\varphi) &:= 1 + \max\{td(\varphi), td(\psi)\}
 \end{aligned}$$

Satz 3.11

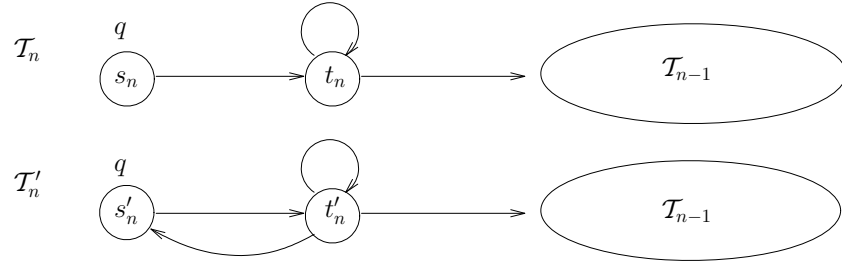
Es gibt keine CTL-Formel φ über einem $\mathcal{P} = \{q, \dots\}$, so dass $\llbracket \varphi \rrbracket = \{(\mathcal{T}, s_0) \mid \text{es gibt einen unendlichen Lauf } s_0, s_1, \dots, \text{ so dass für unendlich viele } i \text{ gilt: } \mathcal{T}, s_i \models q\}$.

Beweis Wir definieren zunächst rekursiv zwei Familien $\mathcal{T}_n, \mathcal{T}'_n$, $n \in \mathbb{N}$ von Transitionssystemen. Der Basisfall mit $n = 0$ ist:

3 Die Logik CTL



Für $n > 1$ sind diese wie folgt definiert.



Sei $M := \{(\mathcal{T}, s) \mid \text{es gibt einen Lauf in } \mathcal{T} \text{ beginnend in } s, \text{ auf dem unendlich oft } q \text{ gilt}\}$. Offensichtlich gilt für alle $n \in \mathbb{N}$: $(\mathcal{T}_n, s_n) \notin M$ aber $(\mathcal{T}'_n, s'_n) \in M$.

Als nächstes zeigen wir per Induktion über den Formelaufbau, dass für alle $n, n' \in \mathbb{N}$ und alle $\varphi \in \text{CTL}$ mit $td(\varphi) \leq \min\{n, n'\}$: $\mathcal{T}_n, x_n \models \varphi$ gdw. $\mathcal{T}'_{n'}, x'_{n'} \models \varphi$, wobei $x \in \{s, t\}$.

Dies sollte klar sein für den atomaren Fall einer Proposition $\varphi = p$, egal ob $p = q$ gilt oder nicht. Die Behauptung folgt sofort aus der Hypothese für die Fälle $\varphi = \psi_1 \vee \psi_2$ und $\varphi = \neg\psi$. Wirklich interessant sind nur die Fälle der temporalen Operatoren.

Fall $\varphi = \text{EX}\psi$. Sei $m := td(\varphi)$, also $td(\psi) = m - 1$ und $n, n' \geq m$. Angenommen, es gilt $\mathcal{T}_n, s_n \models \varphi$. Da t_n der einzige Nachfolger von s_n ist, gilt somit $\mathcal{T}_n, t_n \models \psi$. Wegen der Induktionshypothese angewandt auf t_n und ψ gilt somit auch $\mathcal{T}'_{n'}, t'_n \models \psi$ und somit auch $\mathcal{T}'_{n'}, s'_{n'} \models \varphi$. Die Rückrichtung gilt genauso.

Ebenfalls genauso gezeigt wird die Implikation $\mathcal{T}_n, t_n \models \varphi \Rightarrow \mathcal{T}'_{n'}, t'_{n'} \models \psi$, da alle Transitionen in \mathcal{T} auch in \mathcal{T}' vorhanden sind. Der einzig interessante Fall ist $\mathcal{T}'_{n'}, t'_{n'} \models \varphi$. Somit gibt es einen Nachfolger, der ψ erfüllt. Beachte, dass $t'_{n'}$ drei Nachfolger hat: $t'_{n'}$ selbst, $s'_{n'-1}$ und $s'_{n'}$. Die beiden ersten sind jeweils als t_n bzw. s'_{n-1} auch in \mathcal{T}_n vorhanden. Falls einer von diesen ψ erfüllt, dann gilt wegen der Hypothese, angewandt auf ψ und den entsprechenden Zustand auch $\mathcal{T}_n, t_n \models \varphi$.

Angenommen, es gelte also $\mathcal{T}'_{n'}, s'_{n'} \models \psi$. Beachte, dass die Induktionshypothese für alle $n, n' \geq td(\psi)$ anwendbar ist. Da $n, n' \geq m = td(\psi) + 1$ angenommen wurde, gilt $n - 1 \geq td(\psi)$ und somit auch $\mathcal{T}_n, s_{n-1} \models \psi$. Aber s_{n-1} ist ein Nachfolger von t_n in \mathcal{T} , also gilt dann auch $\mathcal{T}_n, t_n \models \varphi$.

Fall $\varphi = \text{E}(\psi_1 \text{U} \psi_2)$. Betrachte wieder zwei n, n' , so dass $n, n' \geq 1 + \max\{td(\psi_1), td(\psi_2)\}$ gilt. Angenommen, es gilt $\mathcal{T}_n, s_n \models \text{E}(\psi_1 \text{U} \psi_2)$. Dann existiert ein $j \leq n$, so dass entweder

- $\mathcal{T}_n, s_j \models \psi_2$ und für alle i mit $n \geq i > j$: $\mathcal{T}_n, s_i \models \psi_1$ und $\mathcal{T}_n, t_i \models \psi_1$, oder

- $\mathcal{T}_n, t_j \models \psi_2$ und für alle i mit $n \geq i > j$: $\mathcal{T}_n, s_i \models \psi_1$ und $\mathcal{T}_n, t_i \models \psi_1$ und $\mathcal{T}_n, s_j \models \psi_1$.

Zur Vereinfachung nehmen wir an, dass der erste Fall vorliegt. Der zweite wird analog weitergeführt. Wir müssen wiederum eine Fallunterscheidung bzgl. der Ordnung zwischen n' , n und j vornehmen. Sei $n' \leq n$ und $i \leq n'$. Aus der Induktionshypothese, angewandt auf ψ_1 und ψ_2 erhalten wir $\mathcal{T}'_{n'}, s'_{n'} \models \psi_2$. Falls $i < n$, dann beachte, dass $\mathcal{T}'_{n'}$ rekursiv mit Bezug auf $\mathcal{T}'_{n'-1}$ definiert wurde. D.h., i ist zwar eventuell zu klein, um die Induktionshypothese für ψ_i und $\mathcal{T}'_{n'}, s_i$ anzuwenden, aber da offensichtlich $\mathcal{T}'_{n'}, s_i \sim \mathcal{T}_n, s_i$ in diesem Fall gilt, kann aus Bisimulationsinvarianz $\mathcal{T}'_{n'}, s_i \models \psi_1$ geschlossen werden. Dasselbe gilt für alle t_i mit $n' > i \geq j$. Aber dann gilt auch $\mathcal{T}'_{n'}, s'_{n'} \models \mathbf{E}(\psi_1 \mathbf{U} \psi_2)$. Die anderen Fälle, z.B. $n' > n$ etc. werden wiederum analog bewiesen.

Wie im vorherigen Fall gibt es nur einen Unterfall, im dem nicht zu einem Pfad in dem einen Transitionssystem ein entsprechender Pfad in dem anderen vorliegt, der bezeugt, dass φ auch von dem jeweils anderen Zustand erfüllt wird. Dies ist der Fall, wenn $\mathcal{T}'_{n'}, s'_{n'} \models \varphi$ gilt, weil es auf dem Pfad $s'_{n'}, t'_{n'}, s'_{n'}, t'_{n'}, \dots$ einen Zustand gibt, der ψ_2 erfüllt, so dass davor alle ψ_1 erfüllen. Dasselbe gilt genauso, wenn dieser Pfad in $t'_{n'}$ anfängt. Es gibt offensichtlich nur zwei Möglichkeiten: entweder $s'_{n'} \models \psi_2$, oder $t'_{n'} \models \psi_2$ und $s'_{n'} \models \psi_1$. In beiden Fällen lässt sich die Induktionshypothese auf ψ_1 und ψ_2 und die Zustände s_n, t_n, s_{n-1} und t_{n-1} anwenden, um zu zeigen, dass der Lauf $s_n, t_n, s_{n-1}, t_{n-1}, \dots$ die Formel $\psi_1 \mathbf{U} \psi_2$ erfüllt. Somit gilt auch $\mathcal{T}_n, s_n \models \varphi$.

Fall $\varphi = \mathbf{E}(\psi_1 \mathbf{R} \psi_2)$. Wiederum gilt, dass, wenn der entsprechende Pfad in \mathcal{T}_n in s_n oder t_n beginnt, sich leicht ein Pfad in $\mathcal{T}_{n'}$ finden lässt, der zeigt, dass φ auch dort erfüllt ist. Der einzig interessante Fall ist wiederum, dass $\mathcal{T}'_{n'}, s'_{n'} \models \varphi$ (oder genauso $\mathcal{T}'_{n'}, t'_{n'} \models \varphi$) wegen dem Lauf $s'_{n'}, t'_{n'}, s'_{n'}, t'_{n'}, \dots$ gilt. Jetzt benutzen wir die Charakterisierung

$$\mathbf{E}(\psi_1 \mathbf{R} \psi_2) \equiv \mathbf{E}(\psi_2 \mathbf{U} (\psi_1 \wedge \psi_2)) \vee \mathbf{E} \mathbf{G} \psi_2$$

und führen dies auf den obigen U-Fall zurück, falls das linke Disjunkt erfüllt ist. Sei also angenommen, dass das rechte Disjunkt erfüllt ist. Somit gilt also $\mathcal{T}'_{n'}, s'_{n'} \models \psi_2$ und $\mathcal{T}'_{n'}, t'_{n'} \models \psi_2$. Die Induktionshypothese, angewandt auf ψ_2 , liefert dann $\mathcal{T}_n, s_n \models \psi_2$ und $\mathcal{T}_n, t_n \models \psi_2$. Somit gilt auf dem Lauf s_n, t_n, t_n, \dots überall ψ_2 und dann auch $\mathcal{T}_n, s_n \models \varphi$.

Sei nun angenommen, dass es eine CTL-Formel φ gibt, die “es gibt einen Pfad, auf dem unendlich oft q gilt” ausdrückt. Dann hat diese eine feste temporale Tiefe $m := td(\varphi)$. Wegen besagter Eigenschaft müsste dann $M = \llbracket \varphi \rrbracket$ gelten, also $\mathcal{T}_m, s_m \not\models \varphi$ und $\mathcal{T}'_m, s'_m \models \varphi$. Dies steht aber im Widerspruch zu der bewiesenen Aussage, dass \mathcal{T}_m, s_m und \mathcal{T}'_m, s'_m von keiner CTL-Formel unterschieden werden können. Also kann diese Eigenschaft nicht in CTL definierbar sein. ■

3.5 Unäres CTL

In diesem Abschnitt schränken wir die Syntax von CTL auf *unäre*, temporale Operatoren ein, die vorher nur als Ankürzungen definiert wurden.

3 Die Logik CTL

Definition 3.10

Formeln des CTL-Fragments CTL^- über einer Menge \mathcal{P} von Propositionen sind gegeben durch die folgende Grammatik.

$$\varphi ::= q \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \neg\varphi \mid EX\varphi \mid AX\varphi \mid EF\varphi \mid AF\varphi \mid EG\varphi \mid AG\varphi$$

wobei $q \in \mathcal{P}$.

Wir betrachten außerdem noch ein weiteres Fragment von CTL, genannt EF, in dem die Pfadquantoren nur mit dem gleichartigen temporalen Operator verbunden werden. Beachte, dass F implizit einen existentiellen Quantor (über Zustände auf einem Lauf) und G implizit einen universellen Quantor darstellt.

Definition 3.11

Formeln der Logik EF über den Propositionen \mathcal{P} sind gegeben durch die folgende Grammatik.

$$\varphi ::= q \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \neg\varphi \mid EX\varphi \mid AX\varphi \mid EF\varphi \mid AG\varphi$$

wobei $q \in \mathcal{P}$.

Die Semantik von CTL^- , bzw. EF-Formeln ergibt sich eindeutig aus der Semantik der Superlogik CTL.

Satz 3.12

Das Model Checking Problem für CTL^- oder EF ist jeweils P-vollständig.

Beweis Die obere Schranke von P für das Model Checking Problem von CTL überträgt sich trivialerweise auf ihre Fragmente. P-Härte stellt sich laut Satz 2.3 und Satz 3.1 bereits ein, wenn nur die temporalen Operatoren EX und AX vorhanden sind. ■

Satz 3.13

Das Erfüllbarkeitsproblem für CTL^- oder EF ist jeweils EXPTIME-vollständig.

Beweis Die obere Schranke wird wiederum trivialerweise von CTL geerbt. EXPTIME-Härte folgt aus dem Beweis von Satz 3.9, in dem EXPTIME-Härte für das Erfüllbarkeitsproblem von CTL gezeigt wird. Man beachte, dass die in der dortigen Reduktion konstruierten Formeln sämtlich bereits in EF sind. ■

Definition 3.12

Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ ein Transitionssystem und Φ eine Menge von (CTL-)Formeln. Diese induziert wieder in natürlicher Weise eine Äquivalenzrelation \equiv_Φ auf der Menge \mathcal{S} der Zustände von \mathcal{T} , definiert durch

$$s \equiv_\Phi t \quad \text{gdw.} \quad \forall \varphi \in \Phi : \mathcal{T}, s \models \varphi \quad \text{gdw.} \quad \mathcal{T}, t \models \varphi$$

Der *Quotient* von \mathcal{T} und Φ ist das Transitionssystem $\mathcal{T}/\Phi := (\mathcal{S}/\Phi, \rightarrow, \lambda_\Phi)$, wobei

- \mathcal{S}/Φ die Menge aller Äquivalenzklassen von Zuständen in \mathcal{S} unter \equiv_Φ ist, also $\mathcal{S}/\Phi := \{[s]_\Phi \mid s \in \mathcal{S}\}$ und $[s]_\Phi := \{t \in \mathcal{S} \mid s \equiv_\Phi t\}$,

- Transitionen sich einfach auf Äquivalenzklassen übertragen: $[s]_{\Phi} \rightarrow [t]_{\Phi}$ gdw. es $s', t' \in \mathcal{S}$ gibt mit $s \equiv_{\Phi} s'$, $t \equiv_{\Phi} t'$ und $s \rightarrow t$,
- die Zustandsbeschriftungen durch Φ relativiert werden: $\lambda_{\Phi}([s]_{\Phi}) := \lambda(s) \cap \Phi$.

Lemma 3.7

Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ ein Transitionssystem und $\Phi \subseteq \text{CTL}$. Der Quotient \mathcal{T}/Φ ist wohldefiniert.

Beweis Man rechnet leicht nach, dass \equiv_{Φ} eine Äquivalenzrelation auf \mathcal{S} ist. Daher ist die Menge \mathcal{S}/Φ eindeutig. Außerdem sieht man leicht, dass die Definition der Transitionsrelation repräsentantenunabhängig ist: Wenn $[s]_{\Phi} \rightarrow [t]_{\Phi}$ und $s \equiv_{\Phi} s'$, dann auch $[s']_{\Phi} \rightarrow [t]_{\Phi}$.

Es bleibt zu zeigen, dass dies auch für die Beschriftungsfunktion gilt. Seien also $s, s' \in \mathcal{S}$, so dass $s \equiv_{\Phi} s'$, aber $\lambda(s) \cap \Phi \neq \lambda(s') \cap \Phi$. Dann gibt es ein $q \in \Phi$, so dass o.B.d.A. $q \in \lambda(s)$ und $q \notin \lambda(s')$. Dann werden s und s' aber von der atomaren Formel q unterschieden, was im Widerspruch zu der Annahme $s \equiv_{\Phi} s'$ steht. ■

Lemma 3.8

Es gibt ein Transitionssystem \mathcal{T} über einer einelementigen Menge von Propositionen $\mathcal{P} = \{q\}$, so dass für jede endliche Menge $\Phi \subset \text{CTL}$ ein Zustand s existiert, so dass gilt: $\mathcal{T}, s \models \text{AF}q$, aber $\mathcal{T}/\Phi, [s]_{\Phi} \not\models \text{AF}q$.

Beweis Übung. ■

Lemma 3.9

Für alle Transitionssysteme $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$, alle Zustände $s \in \mathcal{S}$, alle $\varphi \in \text{EF}$ und alle Φ mit $\Phi \supseteq \text{Sub}(\varphi)$ gilt: $\mathcal{T}, s \models \varphi$ gdw. $\mathcal{T}/\Phi, [s]_{\Phi} \models \varphi$.

Beweis Um dies per Induktion über den Aufbau von φ zeigen zu können, müssen wir die leicht stärkere Behauptung beweisen, dass \mathcal{T}, s und $\mathcal{T}/\Phi, [s]_{\Phi}$ von keinem $\psi \in \text{Sub}(\varphi)$ unterschieden werden können. Wegen Lemma 3.1 können wir uns auch hier auf Disjunktionen, Negationen und die Konstrukte **EX** und **EF** konzentrieren.

Fall $\psi = q$. Beachte, dass somit $q \in \Phi$ ist. Es gilt $\mathcal{T}, s \models q$ gdw. $q \in \lambda(s)$ gdw. $q \in \lambda(s) \cap \Phi$ gdw. $q \in \lambda_{\Phi}([s]_{\Phi})$ gdw. $\mathcal{T}/\Phi, [s]_{\Phi} \models q$.

Fälle $\psi = \psi_1 \vee \psi_2$ **und** $\psi = \neg\psi'$. Beide folgen sofort aus der Induktionshypothese.

Fall $\psi = \text{EX}\psi'$. Es gilt $\mathcal{T}, s \models \varphi$ gdw. es ein $t \in \mathcal{S}$ gibt mit $s \rightarrow t$ und $t \models \psi'$. Da $\psi' \in \text{Sub}(\varphi)$ wenn $\psi \in \text{Sub}(\varphi)$ können wir hier die Induktionshypothese anwenden und zeigen, dass dies genau dann der Fall ist, wenn $\mathcal{T}/\Phi, [t]_{\Phi} \models \psi'$. Dies ist aber genau dann der Fall, wenn $\mathcal{T}/\Phi, [s]_{\Phi} \models \psi$, da $[s]_{\Phi} \rightarrow [t]_{\Phi}$ gilt.

Fall $\psi = \text{EF}\psi'$. Es gelte $\mathcal{T}, s \models \varphi$. Also gibt es einen Lauf s_0, s_1, \dots mit $s_0 = s$ und ein $k \in \mathbb{N}$, so dass $s_k \models \psi'$. Nach der Induktionshypothese gilt dann auch $\mathcal{T}/\Phi, [s_k]_{\Phi} \models \psi'$. Da $s_i \rightarrow s_{i+1}$ für alle $i \in \mathbb{N}$ gilt auch $[s_i]_{\Phi} \rightarrow [s_{i+1}]_{\Phi}$ für alle $i \in \mathbb{N}$ laut Lemma 3.7. Somit

3 Die Logik CTL

ist $[s_0]_{\Phi}, [s_1]_{\Phi}, \dots$ ein Lauf in \mathcal{T}/Φ und offensichtlich gilt $[s_0]_{\Phi} = [s]_{\Phi}$. Somit gilt aber auch $\mathcal{T}/\Phi, [s]_{\Phi} \models \psi$.

Für die Rückrichtung zeigen wir durch eine separate Induktion, dass für alle $s \in \mathcal{S}$ und alle $k \in \mathbb{N}$ gilt: wenn $\mathcal{T}/\Phi, [s]_{\Phi} \models \mathbf{EF}^k \psi'$, dann gilt $\mathcal{T}, s \models \mathbf{EF} \psi'$.

Für $k = 0$ ist dies trivialerweise wahr, da $\mathbf{EF}^0 \psi' \equiv \mathbf{ff}$. Sei also $k > 0$ und es gelte $\mathcal{T}/\Phi, [s]_{\Phi} \models \mathbf{EF}^k \psi$. Also existiert ein $[t]_{\Phi}$ mit $[s]_{\Phi} \rightarrow [t]_{\Phi}$, so dass $\mathcal{T}/\Phi, [t]_{\Phi} \models \mathbf{EF}^{k-1} \psi$. Nach der Hypothese dieser Nebeninduktion gilt somit $\mathcal{T}, t \models \mathbf{EF} \psi'$. Da $[s]_{\Phi} \rightarrow [t]_{\Phi}$ gilt, existieren s', t' , so dass $s' \rightarrow t'$ und $s' \equiv_{\Phi} s$ und $t' \equiv_{\Phi} t$. Wegen letzterem gilt somit auch $\mathcal{T}, t' \models \mathbf{EF} \psi'$ und dann auch $\mathcal{T}, s' \models \mathbf{EF} \psi'$. Da aber $s \equiv_{\Phi} s'$ und $\mathbf{EF} \psi' \in \Phi$ gilt somit auch $\mathcal{T}, s \models \mathbf{EF} \psi'$.

Sei nun also angenommen, dass $\mathcal{T}/\Phi, [s]_{\Phi} \models \mathbf{EF} \psi'$ gilt. Also existiert ein Lauf $[s_0]_{\Phi}, [s_1]_{\Phi}, \dots$ mit $[s_0]_{\Phi} = [s]_{\Phi}$ und ein $k \in \mathbb{N}$, so dass $\mathcal{T}_{\Phi}, [s_k]_{\Phi} \models \psi'$ gilt. Dann gilt aber auch $\mathcal{T}, [s_k]_{\Phi} \models \mathbf{EF}^{k+1} \psi'$ und nach der in der Nebeninduktion bewiesenen Behauptung gilt dann $\mathcal{T}, s \models \psi$, was zu beweisen war. ■

Mithilfe dieses Lemmas lässt sich jetzt einerseits die kleine Modelleigenschaft für EF zeigen, sowie EF von CTL^- bzgl. Ausdrucksstärke trennen.

Satz 3.14

Für alle $\varphi \in \text{EF}$ gilt: Wenn φ erfüllbar ist, dann hat es ein Modell der Größe höchstens $2^{|\varphi|}$.

Beweis Angenommen φ ist erfüllbar, es gibt also ein Transitionssystem $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda, s)$, so dass $\mathcal{T}, s \models \varphi$ gilt. Nach Lemma 3.7 existiert dann auch das Transitionssystem $\mathcal{T}/\text{Sub}(\varphi)$, und wegen Lemma 3.9 gilt auch $\mathcal{T}/\text{Sub}(\varphi), [s]_{\text{Sub}(\varphi)} \models \varphi$.

Es bleibt zu zeigen, dass die Größe von $\mathcal{T}/\text{Sub}(\varphi)$ durch $2^{|\varphi|}$ beschränkt ist. Angenommen, dem sei nicht so. Sei $n := 2^{|\varphi|}$. Dann gibt es mindestens $n + 1$ verschiedene Zustände $[s_0]_{\text{Sub}(\varphi)}, \dots, [s_n]_{\text{Sub}(\varphi)}$ in $\mathcal{T}/\text{Sub}(\varphi)$. Dann gibt es aber auch $n + 1$ Zustände s_0, \dots, s_n in \mathcal{T} , so dass für alle $0 \leq i < j \leq n$ gilt: $s_i \not\equiv_{\text{Sub}(\varphi)} s_j$. Also existieren für alle $0 \leq i < j \leq n$ jeweils ein $\psi \in \text{Sub}(\varphi)$, so dass o.B.d.A. $s_i \models \psi$ und $s_j \not\models \psi$ gilt. Dies ist aber unmöglich, denn es gibt insgesamt nur $2^{|\varphi|}$ viele Teilmengen von $\text{Sub}(\varphi)$. Also muss es $i, j \in \{0, \dots, n\}$ geben, so dass $i \neq j$ und für alle $\psi \in \text{Sub}(\varphi)$: $s_i \models \psi$ gdw. $s_j \models \psi$. Somit gibt es also i, j mit $i \neq j$ und $s_i \equiv_{\text{Sub}(\varphi)} s_j$. ■

Satz 3.15

$\text{EF} \preceq \text{CTL}^-$.

Beweis Trivialerweise lässt sich jede EF-definierbare Eigenschaft in CTL^- ausdrücken, da EF ein syntaktisches Fragment von CTL^- ist. Zur Striktheit dieser Einbettung zeigen wir, dass es keine EF-Formel gibt, die äquivalent zu der CTL^- -Formel $\mathbf{AF}q$ ist.

Angenommen, dem wäre nicht so. Dann gibt es also ein $\varphi \in \text{EF}$, so dass $\varphi \equiv \mathbf{AF}q$. Da $|\text{Sub}(\varphi)| < \infty$, gibt es laut Lemma 3.8 ein Transitionssystem \mathcal{T} mit einem Zustand s , so dass nicht gilt: $\mathcal{T}, s \models \varphi$ gdw. $\mathcal{T}/\text{Sub}(\varphi), [s]_{\text{Sub}(\varphi)} \models \varphi$. Dies steht aber im Widerspruch zu Lemma 3.9, welches besagt, dass keine EF-Formel φ ein Transitionssystem und dessen Quotienten bzgl. $\text{Sub}(\varphi)$ unterscheiden kann. ■

3 Die Logik CTL

Worten: Der Beweis kann genauso geführt werden wie im obigen Fall, beginnend mit der Annahme, dass $\mathcal{T}_{n,m}, 0 \not\models \varphi$ gilt, usw.

Die Behauptung des Satzes wird dann wieder in der üblichen Weise bewiesen. Angenommen, es gäbe ein $\varphi \in \text{CTL}^-$, so dass $\varphi \equiv \mathbf{E}(p\mathbf{U}q)$. Sei $n := td(\varphi)$. Dann gilt einerseits $\mathcal{T}_{n,n}, 0 \models \varphi$ und $\mathcal{T}'_{n,n} \not\models \varphi$ wegen besagter Äquivalenz. Andererseits wurde soeben bewiesen, dass dann aber auch $\mathcal{T}_{n,n}, 0 \models \varphi$ gdw. $\mathcal{T}'_{n,n} \models \varphi$ gelten müsste. ■

Im Gegensatz zu den vorher konstruierten Transitionssystemen, sind die zur Trennung von CTL^- und CTL benutzten $\mathcal{T}_{n,m}$ und $\mathcal{T}'_{n,m}$ unendlich groß. Somit folgt nicht sofort, dass die Separationsresultate wie die zwischen HML und CTL z.B. auch auf der eingeschränkten Klasse aller endlichen Transitionssysteme gelten. Man sieht aber leicht, dass $\mathcal{T}_{n,m}$ und $\mathcal{T}'_{n,m}$ jeweils bisimilar zu einem Transitionssystem der Größe $n + 2m$ sind, welche eine Schleife der Länge $2m$ bilden, in die ein Pfad der Länge n führt.

Eine andere Möglichkeit, zu zeigen, dass es CTL-Formeln gibt, zu denen keine CTL^- -Formel äquivalent auf der Klasse aller endlichen Transitionssysteme ist, bietet Satz 3.16 zusammen mit der endlichen Modelleigenschaft für CTL (Korollar 3.3). Angenommen, jede CTL-Formel φ ist äquivalent zu einer CTL^- -Formel φ' über der Klasse aller endlichen Transitionssysteme, aber es gibt eine CTL-Formel φ_0 , die nicht äquivalent zu einer CTL^- -Formel über der Klasse aller Transitionssysteme ist. Dann muss φ_0 erfüllbar sein, denn ansonsten wäre $\models \neg\varphi_0$, also $\varphi_0 \equiv \mathbf{ff}$. Aber \mathbf{ff} ist in CTL^- sicherlich ausdrückbar.

Da φ_0 und φ'_0 über der Klasse aller endlichen Transitionssysteme äquivalent, über der Klasse aller unendlichen Transitionssysteme aber nicht äquivalent sind, gibt es ein \mathcal{T} mit Zustandsmenge \mathcal{S} , $|\mathcal{S}| = \infty$, und ein $s \in \mathcal{S}$, so dass $\mathcal{T}, s \models \varphi_0$ und $\mathcal{T}, s \models \neg\varphi'_0$. Also gilt $\mathcal{T}, s \models \varphi_0 \wedge \neg\varphi'_0$.

Andererseits gilt jedoch für jedes endliche \mathcal{T}' mit Zustandsmenge \mathcal{S}' und jedem $s' \in \mathcal{S}'$: $\mathcal{T}', s' \models \varphi_0$ gdw. $\mathcal{T}', s' \models \varphi'_0$, und damit dann auch $\mathcal{T}', s' \not\models \varphi_0 \wedge \neg\varphi'_0$.

Aber $\varphi_0 \wedge \neg\varphi'_0 \in \text{CTL}$, und CTL hat die endliche Modelleigenschaft laut Korollar 3.3. Dies steht aber im Widerspruch zu der Tatsache, dass $\varphi_0 \wedge \neg\varphi'_0$ nur in einem unendlichen Modell erfüllt ist.