4 Die Logik LTL

In Kapitel 3, genauer in Abschnitt 3.4 haben wir angedeutet, dass CTL auf linearer Modellen spezielle Eigenschaften hat. So drückt z.B. die CTL-Formel $\mathtt{EGEF}q$ durchaus auf linearen Modellen aus, dass q unendlich oft gelten muss. Dies liegt offensichtlich daran, dass dem existentiellen Pfadquantor $\mathtt{E}$ keine Bedeutung zukommt, denn es gibt in jedem Zustand genau einen ausgehenden Lauf.

Auch kann man sich vorstellen, dass das Erfüllbarkeitsproblem für CTL auf linearen Modellen evtl. einfacher ist, denn die Regel ($\mathtt{X}$), welche als einzige mehrere Prämissen in den allgemeinen Erfüllbarkeitstableaux für CTL hat, würde auf linearen Modellen ebenfalls nur eine Prämisse haben.

Um solche Effekte genauer zu untersuchen, betrachten wir die Linearzeitlogik LTL. Diese wurde im übrigen von Pnueli für die Verifikation von Programmen bereits 1977 vorgeschlagen [Pnu77] und von Kamp in der Philosophie noch früher benutzt [Kam68]. CTL hingegen wurde erst Anfang der 80er Jahre von Clarke und Emerson vorgestellt [CE81]. Vorausgegangen waren Arbeiten über *branching time* Logiken z.B. von Ben-Ari, Manna und Pnueli [BAPM83].

4.1 Syntax und Semantik

Definition 4.1
Sei $\mathcal{P}$ wieder eine höchstens abzählbar unendlich große Menge von Propositionen. Formeln der Logik LTL über $\mathcal{P}$ sind gegeben durch folgende Grammatik.

$$\varphi \ ::= \ q \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \neg\varphi \mid \mathtt{X}\varphi \mid \varphi\mathtt{U}\varphi \mid \varphi\mathtt{R}\varphi$$

Wir verwenden (wieder) die folgenden Abkürzungen: $\mathtt{tt} := q \vee \neg q$ für ein beliebiges $q \in \mathcal{P}$, $\mathtt{ff} := \neg\mathtt{tt}$, $\mathtt{F}\varphi := \mathtt{tt}\mathtt{U}\varphi$ und $\mathtt{G}\varphi := \mathtt{ff}\mathtt{R}\varphi$.

Wie bei CTL definieren wir wegen den Charakterisierungen der temporalen Operaten als Fixpunkte eine erweiterte Unterformelmenge.

Definition 4.2
Sei $\varphi \in$ LTL. Die *erweiterte Unterformelmenge* $Sub^*(\varphi)$ von φ ist induktiv definiert wie

folgt.

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

LTL wird zwar genauso wie CTL über totalen, knotenbeschrifteten Transitionssystemen interpretiert. Im Gegensatz zu CTL ist hier die Modellbeziehung jedoch eine Relation zwischen Läufen eines solchen Transitionssystems und einer Formel.

Definition 4.3
Sei $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ ein totales, knotenbeschriftetes Transitionssystem. Wenn $\pi = s_0 s_1 \ldots$ ein Lauf in $\mathcal{T}$ ist, dann bezeichnet $\pi^{(i)}$ für ein $i \in \mathbb{N}$ das i-te Suffix $s_i s_{i+1} \ldots$ von π.

Die Semantik von LTL ist induktiv definiert wie folgt.

$$\begin{aligned}
\mathcal{T}, \pi \models q \quad &\text{gdw.} \quad \pi = s_0 \ldots \text{ und } q \in \lambda(s_0) \\
\mathcal{T}, \pi \models \varphi \vee \psi \quad &\text{gdw.} \quad \mathcal{T}, \pi \models \varphi \text{ oder } \mathcal{T}, \pi \models \psi \\
\mathcal{T}, \pi \models \varphi \wedge \psi \quad &\text{gdw.} \quad \mathcal{T}, \pi \models \varphi \text{ und } \mathcal{T}, \pi \models \psi \\
\mathcal{T}, \pi \models \neg\varphi \quad &\text{gdw.} \quad \mathcal{T}, \pi \not\models \varphi \\
\mathcal{T}, \pi \models \mathtt{X}\varphi \quad &\text{gdw.} \quad \mathcal{T}, \pi^{(1)} \models \varphi \\
\mathcal{T}, \pi \models \varphi \mathtt{U} \psi \quad &\text{gdw.} \quad \exists k \in \mathbb{N} \text{ mit } \mathcal{T}, \pi^{(k)} \models \varphi \text{ und } \forall j < k : \mathcal{T}, \pi^{(j)} \models \psi \\
\mathcal{T}, \pi \models \varphi \mathtt{R} \psi \quad &\text{gdw.} \quad \forall k \in \mathbb{N} : \mathcal{T}, \pi^{(k)} \models \varphi \text{ oder } \exists j < k : \mathcal{T}, \pi^{(j)} \models \psi
\end{aligned}$$

Definiere $[\![\varphi]\!]^\pi := \{\pi^{(i)} \mid i \in \mathbb{N} \text{ und } \mathcal{T}, \pi^{(i)} \models \varphi\}$ für einen Lauf π in $\mathcal{T}$ und $[\![\varphi]\!]^{\mathcal{T}} := \{\pi \mid \pi$ ist Lauf in $\mathcal{T}$ und $\mathcal{T}, \pi \models \varphi\}$.

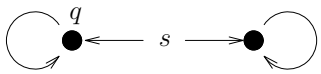
Für ein $s \in \mathcal{S}$ definieren wir außerdem: $\mathcal{T}, s \models \varphi$ gdw. $\mathcal{T}, \pi \models \varphi$ für alle Läufe $\pi = s \ldots$ gilt.

Der letzte Teil dieser Definition wird es uns später ermöglichen, die Logiken CTL und LTL miteinander zu vergleichen. Andererseits verlangt er aber, dass man die beiden verschiedenen Modellbeziehungen $s \models \varphi$ und $\pi \models \varphi$ strikt trennt, wie folgende Überlegung zeigt.

LTL ist offensichtlich unter Komplement abgeschlossen bzgl. der Laufmodellbeziehung, denn für alle $\varphi \in$ LTL und alle Läufe π eines Transitionssystems $\mathcal{T}$ gilt:

$$\mathcal{T}, \pi \models \varphi \quad \text{gdw.} \quad \mathcal{T}, \pi \not\models \neg\varphi$$

Bezgl. der Zustandsmodellbeziehung ist LTL jedoch nicht unter Komplement abgeschlossen. Betrachte die Formel $\varphi := \mathtt{X}q$ und ihr Komplement (bzgl. der Laufmodellbeziehung) $\neg\varphi$. Für den Zustand s des Transitionssystems



gilt: $s \not\models \varphi$ und $s \not\models \neg\varphi$. Es gibt also Zustände, die weder eine gegebene Formeln noch ihr Komplement erfüllen. Beachte, dass es jedoch für einen Zustand unmöglich ist, sowohl eine Formel als auch ihr Komplement zu erfüllen.

Lemma 4.1
Für alle totale, knotenbeschriftete Transitionssysteme $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$, alle $s \in \mathcal{S}$ und alle $\varphi \in$ LTL gilt höchstens eine der beiden Beziehungen $\mathcal{T}, s \models \varphi$ und $\mathcal{T}, s \models \neg\varphi$.

Beweis Angenommen, es gäbe ein $\varphi \in$ LTL und ein Transitionssystem $\mathcal{T}$ mit Zustand s, so dass $\mathcal{T}, s \models \varphi$ und $\mathcal{T}, s \models \neg\varphi$ gilt. Da $\mathcal{T}$ implizit als total angenommen wird, gibt es mindestens einen Lauf $\pi = s \ldots$ in $\mathcal{T}$. Wegen $\mathcal{T}, s \models \varphi$ gilt somit $\mathcal{T}, \pi \models \varphi$, und wegen $\mathcal{T}, s \models \neg\varphi$ gilt auch $\mathcal{T}, \pi \models \neg\varphi$. Dies ist aber wegen der Semantik von LTL ausgeschlossen. ■

Da die Laufmodellbeziehung somit natürlicher ist als die Zustandsmodellbeziehung, benutzen wir diese, wenn wir über Äquivalenz ($\varphi \equiv \psi$ gdw. wenn für alle π: $\pi \models \varphi$ gdw. $\pi \models \psi$), Erfüllbarkeit (Gibt es ein π, so dass $\pi \models \varphi$?) und Allgemeingültigkeit sprechen. Ein weiterer Grund dafür ist, dass eine LTL-Formeln von einem Lauf $\pi = s \ldots$ erfüllt wird, gdw. sie von s in dem Transitionssystem, welches nur den Lauf π hat, erfüllt wird.

Lemma 4.2
In LTL gelten die folgenden Äquivalenzen.

a) $\neg\mathtt{X}\varphi \equiv \mathtt{X}\neg\varphi$,

b) $\neg(\varphi \mathtt{U} \psi) \equiv (\neg\varphi)\mathtt{R}(\neg\psi)$,

c) $\mathtt{X}(\varphi \vee \psi) \equiv \mathtt{X}\varphi \vee \mathtt{X}\psi$,

d) $\mathtt{X}(\varphi \wedge \psi) \equiv \mathtt{X}\varphi \wedge \mathtt{X}\psi$.

Beweis Übung. ■

Man sieht somit leicht, dass wir uns – wie im Fall von HML oder CTL – auf Formeln beschränken können, die nur mit den folgenden Konstrukten gebildet werden:

- atomaren Propositionen, Disjunktionen, Negationen und den temporalen Operatoren `X` und `U`, oder
- atomaren Propositionen und ihren Negationen, Disjunktionen, Konjunktionen und den temporalen Operatoren `X`, `U` und `R`.

Im zweiten Fall sprechen wir wieder von *positiver Normalform*.

4.2 Beispiele

Beispiel 4.1
Im vorigen Kapitel haben wir gesehen, dass man in CTL nicht "es gibt einen Lauf, auf dem unendlich oft q gilt" ausdrücken kann. Der Grund war, dass in CTL jeder temporale Operator `X`, `U` oder `R` unmittelbar auf einen Pfadquantor `E` oder `A` folgen muss. Dies ist in LTL nicht der Fall. So läßt sich leicht ausdrücken, dass auf einem *gegebenen* Pfad q unendlich oft gilt: $\texttt{GF}q$.

Über Zuständen interpretiert besagt diese Formel jedoch, dass auf *allen* Läufen q unendlich oft gilt. Dies war in CTL ebenfalls möglich. Die obige Eigenschaft ist in LTL offensichtlich nicht ausdrückbar, denn über Zuständen interpretiert ist jede Formel implizit allquantifizert. Es ist jedoch möglich, das Komplement der obigen Eigenschaft in LTL auszudrücken. Dazu negieren wir einfach die LTL-Formel, die auf einem gegebenen Lauf die gewünschte Eigenschaft formalisiert: $\texttt{FG}\neg q$ besagt, dass q nur endlich oft gilt. Somit gilt $s \not\models \texttt{FG}\neg q$ gdw. es einen Lauf ausgehend aus s gibt, auf dem q unendlich oft gilt.

Beispiel 4.2
Zum Vergleich mit CTL betrachten wir wieder das Beispiel 3.2 der Spezifikation einer Ampel. Die zugrundeliegenden Propositionen sind wiederum $A := \{\texttt{arot}, \texttt{arotgelb}, \texttt{agruen}, \texttt{agelb}\}$ und $\texttt{frot}, \texttt{fgruen}, \texttt{gedrueckt}$. Da es in LTL nicht möglich ist zu sagen, dass es immer einen Lauf gibt, ändern wir die Spezifikation im letzten Teil folgendermaßen ab.

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. Wenn sie rot ist, ist sie danach immer noch rot oder rotgelb, wenn sie grün ist, ist sie danach immer noch grün oder gelb.

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 wird immer wieder gedrückt.

Dies lässt sich in LTL folgendermaßen ausdrücken.

$$
\begin{aligned}
\varphi_{Ampel} \;:=\; & \texttt{frot} \wedge \texttt{arot} \wedge \texttt{XG}\neg(\texttt{frot} \wedge \texttt{arot}) \wedge \\
& \texttt{G}\Big((\texttt{fgruen} \leftrightarrow \neg\texttt{frot}) \wedge \big(\bigvee_{q \in A} q\big) \wedge \big(\bigwedge_{p,q \in A, p \neq q} \neg(p \wedge q)\big) \\
& \quad \wedge \; \big((\texttt{agelb} \rightarrow \texttt{Xarot}) \wedge (\texttt{arotgelb} \rightarrow \texttt{Xagruen}) \wedge \\
& \qquad (\texttt{arot} \rightarrow \texttt{X}(\texttt{arot} \vee \texttt{arotgelb})) \wedge (\texttt{agruen} \rightarrow \texttt{X}(\texttt{agruen} \vee \texttt{agelb}))\big) \\
& \quad \wedge \; \big((\texttt{fgruen} \rightarrow \texttt{arot}) \wedge (\texttt{agruen} \rightarrow \texttt{frot})\big) \\
& \quad \wedge \; (\texttt{fgruen} \rightarrow \texttt{Xfrot}) \\
& \quad \wedge \; \big(\texttt{gedrueckt} \rightarrow (\texttt{frot U } (\texttt{fgruen} \wedge \neg\texttt{gedrueckt}))\big) \\
& \quad \wedge \; \texttt{Fgedrueckt} \;\Big)
\end{aligned}
$$

4.3 Fixpunktcharakterisierungen

Wie in CTL lassen sich die temporalen Operatoren `U` und `R` wieder als Fixpunkte einer bestimmten Gleichung über LTL-Formeln auffassen.

Lemma 4.3
Für alle $\varphi, \psi \in$ LTL gilt:.

a) $\varphi \texttt{U} \psi \equiv \psi \vee (\varphi \wedge \texttt{X}(\varphi \texttt{U} \psi))$,

b) $\varphi \texttt{R} \psi \equiv \psi \wedge (\varphi \vee \texttt{X}(\varphi \texttt{R} \psi))$

Beweis Übung. ∎

Die jeweils rechte Seite einer dieser Gleichung bezeichnen wir wiederum als *Abwicklung* von $\varphi \texttt{U} \psi$ bzw. von $\varphi \texttt{R} \psi$. Wie im Fall von CTL benutzen wir auch wieder Formeln mit Formelvariablen, z.B. $\varphi(\alpha)$, welche über eine *Umgebung* z.B. in der Form $[\![\varphi(\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto P]}$ interpretiert werden. Dies erlaubt es uns, über Fixpunkte von solchen offenen Formeln zu sprechen.

Das nächste Lemma verdeutlicht den semantischen Unterschied zwischen einem `U` und einem `R`. Beide sind Fixpunkte der jeweiligen Gleichung, beim `U` handelt es sich jedoch um den *kleinsten Fixpunkt* dieser Gleichung, beim `R` um den *größten Fixpunkte* der anderen Gleichung. Dabei ist *kleinst/größt* mengentheoretisch zu verstehen: A ist die kleinste Menge, die eine Bedingung erfüllt gdw. für alle Mengen B, die ebenfalls diese Bedingung erfüllen, $A \subseteq B$ gilt, usw.

Lemma 4.4
Sei $\mathcal{T}$ ein Transitionssystem, Π die Menge aller Läufe in $\mathcal{T}$ und $\varphi, \psi \in$ LTL. Für alle $P \subseteq \Pi$ gilt:

a) Wenn $[\![\psi \vee (\varphi \wedge \texttt{X}\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto P]} \subseteq P$, dann gilt $[\![\varphi \texttt{U} \psi]\!]^{\mathcal{T}} \subseteq P$.

b) Wenn $P \subseteq [\![\psi \wedge (\varphi \vee \texttt{X}\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto P]}$, dann gilt $P \subseteq [\![\varphi \texttt{R} \psi]\!]^{\mathcal{T}}$.

Beweis (a) Sei $P \subseteq \Pi$ gegeben und es gelte $[\![\psi \vee (\varphi \wedge \mathtt{X}\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto P]} \subseteq P$. Wir müssen $[\![\varphi \mathtt{U} \psi]\!]^{\mathcal{T}} \subseteq P$ zeigen.

Für jedes $k \in \mathbb{N}$ sei $P_k := \{\pi \in \Pi \mid \pi^{(k)} \models \psi$ und für alle $j < k$ gilt $\pi^{(j)} \models \varphi\ \}$. Man sieht leicht, dass gilt:

$$[\![\varphi \mathtt{U} \psi]\!]^{\mathcal{T}} \;=\; \bigcup_{k \in \mathbb{N}} P_k$$

Somit reicht es aus zu zeigen, dass für alle $k \in \mathbb{N}$ gilt: $P_k \subseteq P$. Dies beweisen wir durch Induktion über k.

Fall $k = 0$. Sei $\pi \in P_0$, also $\pi \models \psi$. Somit gilt dann auch $\pi \in [\![\psi \vee (\varphi \wedge \mathtt{X}\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto P]}$ und nach Voraussetzung gilt somit $\pi \in P$.

Fall $k > 0$. Sei $\pi \in P_k$, also $\pi^{(k)} \models \psi$ und $\pi^{(j)} \models \varphi$ für alle $j < k$. Insbesondere gilt $\pi \models \varphi$, da $\pi = \pi^{(0)}$. Darüberhinaus gilt $\pi^{(1)} \in P_{k-1}$ und somit $\pi^{(1)} \in P$ nach Induktionsvoraussetzung. Dann gilt aber auch $\pi \in [\![\varphi \wedge \mathtt{X}\alpha]\!]^{\mathcal{T}}_{[\alpha \mapsto P]}$ bzw. sogar $\pi \in [\![\psi \vee (\varphi \wedge \mathtt{X}\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto P]}$. Nach Voraussetzung ist dann auch $\pi \in P$.

(b) Dies kann entweder genauso bewiesen werden, indem man Mengen P_k von Läufen definiert, die $\varphi \mathtt{R} \psi$ *nicht* erfüllen, weil das k-te Suffix ψ nicht erfüllt. Dann zeigt man, dass unter besagter Voraussetzung und wiederum durch Induktion P enthalten ist im Durchschnitt aller P_k.

Andererseits kann die Behauptung aber auch folgendermaßen bewiesen werden.

$$\begin{aligned}
P \;\subseteq\; [\![\psi \wedge (\varphi \vee \mathtt{X}\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto P]} \quad & \Leftrightarrow \quad \Pi \setminus [\![\psi \wedge (\varphi \vee \mathtt{X}\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto P]} \;\subseteq\; \Pi \setminus P \\
& \Leftrightarrow \quad [\![\neg(\psi \wedge (\varphi \vee \mathtt{X}\alpha))]\!]^{\mathcal{T}}_{[\alpha \mapsto P]} \;\subseteq\; \Pi \setminus P \\
& \Leftrightarrow \quad [\![\neg\psi \vee (\neg\varphi \wedge \mathtt{X}\neg\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto P]} \;\subseteq\; \Pi \setminus P \\
& \Leftrightarrow \quad [\![\neg\psi \vee (\neg\varphi \wedge \mathtt{X}\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto \Pi \setminus P]} \;\subseteq\; \Pi \setminus P \\
& \Rightarrow \quad [\![\neg\varphi \mathtt{U} \neg\psi]\!]^{\mathcal{T}} \;\subseteq\; \Pi \setminus P \\
& \Leftrightarrow \quad P \;\subseteq\; [\![\neg(\neg\varphi \mathtt{U} \neg\psi)]\!]^{\mathcal{T}} \\
& \Leftrightarrow \quad P \;\subseteq\; [\![\varphi \mathtt{R} \psi)]\!]^{\mathcal{T}}
\end{aligned}$$

wobei Teil (a) und Lemma 4.2 benutzt werden. ∎

Lemma 4.4 stellt ein Hifsmittel zur Verfügung, mit dem man z.B. Formeln der Form $\chi \to \varphi \mathtt{R} \psi$ oder $\varphi \mathtt{U} \psi \to \chi$ als allgemeingültig zeigen kann. Dazu muss man im ersten Fall lediglich $\chi \to \psi \wedge (\varphi \vee \mathtt{X}\chi)$ bzw. im zweiten Fall $\psi \vee (\varphi \wedge \mathtt{X}\chi) \to \chi$ zeigen.

Beispiel 4.3

Wir wollen zeigen, dass in LTL $\models (\mathtt{X}\varphi)\mathtt{U}(\mathtt{X}\psi) \to \mathtt{X}(\varphi \mathtt{U} \psi)$ gilt. Wegen Lemma 4.4 reicht es aus zu zeigen, dass $\mathtt{X}(\varphi \mathtt{U} \psi)$ ein Prä-Fixpunkt der Abwicklung von $(\mathtt{X}\varphi)\mathtt{U}(\mathtt{X}\psi)$ ist, d.h. dass gilt:

$$\models \mathtt{X}\psi \vee (\mathtt{X}\varphi \wedge \mathtt{XX}(\varphi \mathtt{U} \psi)) \to \mathtt{X}(\varphi \mathtt{U} \psi)$$

Lemma 4.2 besagt, dass der X-Operator mit den booleschen Operatoren kommutiert, d.h. dass $\mathtt{X}\psi \vee (\mathtt{X}\varphi \wedge \mathtt{X}\chi) \equiv \mathtt{X}(\psi \vee (\varphi \wedge \chi))$ gilt. Also reicht es aus zu zeigen, dass

$$\models \mathtt{X}(\psi \vee (\varphi \wedge \mathtt{X}(\varphi \mathtt{U} \psi))) \to \mathtt{X}(\varphi \mathtt{U} \psi)$$

gilt, was aber wiederum sofort aus Lemma 4.3 folgt.

Um gegenteilige Aussagen der Form $\chi \to \varphi \mathtt{U} \psi$ zu zeigen, bieten sich wiederum Approximanden an.

Definition 4.4
Für alle $\varphi, \psi \in$ LTL definieren wir *Approximanden* einer Formel $\varphi \mathtt{U} \psi$ bzw. $\varphi \mathtt{R} \psi$ für alle $k \in \mathbb{N}$ wie folgt.

$$\begin{array}{llll} \varphi \mathtt{U}^0 \psi & := & \mathtt{ff} & \varphi \mathtt{U}^{k+1} \psi \quad := \quad \psi \vee (\varphi \wedge \mathtt{X}(\varphi \mathtt{U}^k \psi)) \\ \varphi \mathtt{R}^0 \psi & := & \mathtt{tt} & \varphi \mathtt{R}^{k+1} \psi \quad := \quad \psi \wedge (\varphi \vee \mathtt{X}(\varphi \mathtt{R}^k \psi)) \end{array}$$

Lemma 4.5
Für alle totalen Transitionssysteme und alle $\varphi, \psi \in$ LTL gilt:

a) $[\![\varphi \mathtt{U} \psi]\!]^{\mathcal{T}} = \bigcup_{k \in \mathbb{N}} [\![\varphi \mathtt{U}^k \psi]\!]^{\mathcal{T}}$,

b) $[\![\varphi \mathtt{R} \psi]\!]^{\mathcal{T}} = \bigcap_{k \in \mathbb{N}} [\![\varphi \mathtt{R}^k \psi]\!]^{\mathcal{T}}$.

Beweis (a) Die Richtung "$\supseteq$" wird wie in Lemma 3.5 durch Induktion über k bewiesen. Für die Richtung "$\subseteq$" benutzen wir das soeben bewiesene Lemma 4.4. Demnach reicht es aus zu zeigen, dass $\bigcup_{k \in \mathbb{N}} [\![\varphi \mathtt{U}^k \psi]\!]^{\mathcal{T}}$ ein Prä-Fixpunkt von der Abwicklung von $\varphi \mathtt{U} \psi$ ist. Sei $P_k := [\![\varphi \mathtt{U}^k \psi]\!]^{\mathcal{T}}$. Da $\varphi \mathtt{U}^0 \psi = \mathtt{ff}$, gilt offensichtlich $\bigcup_{k \in \mathbb{N}} P_k = \bigcup_{k \geq 1} P_k$. Außerdem gilt: wenn $\pi^{(1)} \in P_k$ und $\pi \models \varphi$ dann $\pi \in P_{k+1}$. Jetzt gilt

$$\begin{array}{rcl} [\![\psi \vee (\varphi \wedge \mathtt{X}\alpha)]\!]^{\mathcal{T}}_{[\alpha \mapsto \bigcup_{k \in \mathbb{N}} P_k]} & = & [\![\psi]\!]^{\mathcal{T}} \cup ([\![\varphi]\!]^{\mathcal{T}} \cap \{\pi \mid \pi^{(1)} \in P_k \text{ für ein } k \in \mathbb{N}\}) \\ & \subseteq & [\![\psi]\!]^{\mathcal{T}} \cup \bigcup_{k \geq 1} P_k \quad = \quad \bigcup_{k \geq 1} P_k \quad = \quad \bigcup_{k \in \mathbb{N}} P_k \end{array}$$

da $[\![\psi]\!]^{\mathcal{T}} \subseteq P_1$. Aus Lemma 4.4 folgt dann sofort die Behauptung.

(b) Folgt dann aus Teil (a) und Lemmas 4.2 und 4.3. ∎

4.4 Ausdrucksstärke

Satz 4.1
Über Zuständen von Transitionssystemen interpretiert gilt:

a) CTL $\not\leq$ LTL,

b) LTL $\not\leq$ CTL.

Beweis (a) Betrachte die CTL-Formel $\mathtt{EX}q$. Angenommen, es gäbe eine LTL-Formel φ, so dass für alle Zustände eines beliebigen Transitionssystems gilt: $s \models \mathtt{EX}q$ gdw. $s \models \varphi$, d.h. für alle Läufe $\pi = s \ldots$ gilt $\pi \models \varphi$. Wir unterscheiden drei Fälle.

1. φ ist erfüllbar, aber $\neg\varphi$ ist nicht erfüllbar. Also gilt $\models \varphi$. Betrachte nun das Transitionssystem, welches nur aus einem Zustand s mit Beschriftung $\emptyset$ und der Transition $s \to s$ besteht. Offensichtlich gilt $s \models \varphi$, aber $s \not\models \mathtt{EX}q$.

2. φ ist unerfüllbar, aber $\neg\varphi$ ist erfüllbar. Also gilt $\models \neg\varphi$. Betrachte genauso ein Transitionssystem mit Zustand s, Beschriftung $\lambda(s) = \{q\}$ und Transition $s \to s$. Hier gilt $s \models \mathtt{EX}q$, aber offensichtlich $s \not\models \varphi$.

3. Sowohl φ als auch $\neg\varphi$ sind erfüllbar. Dann gibt es einen Lauf $\pi = s_0 s_1 \ldots$, so dass $\pi \not\models \varphi$. Betrachte nun das Transitionssystem, welches den Lauf π um einen Zustand t mit Beschriftung $\lambda(t) = \{q\}$ und den Transitionen $s_0 \to t$ und $t \to t$ erweitert. Somit gibt es (mindestens) zwei Läufe: π und $\pi' := s_0\, t\, t \ldots$. Da $\pi \not\models \varphi$ gilt auch $s \not\models \varphi$. Andererseits gilt aber $s \models \mathtt{EX}q$ wegen π'.

Somit ist gezeigt, dass es eine CTL-Formel gibt, zu der keine LTL-Formel äquivalent über Zuständen ist. Beachte, dass eine Formel φ und ihr Komplement $\neg\varphi$ nicht beide gleichzeitig unerfüllbar sein können. Denn dann würde auch gelten $\models \varphi$ und $\models \neg\varphi$, womit auch $\models \varphi \wedge \neg\varphi$ bzw. $\models \mathtt{ff}$ gelten würde.

(b) Betrachte die LTL-Formel $\mathtt{FG}\neg q$. Angenommen, es gäbe eine CTL-Formel φ, so dass für alle Zustände s eines Transitionssystems gilt $s \models \varphi$ gdw. $s \models \mathtt{FG}\neg q$. Dann wäre aber auch $\neg\varphi$ eine CTL-Formel. Und diese würde besagen: "es gibt einen Pfad, auf dem unendlich oft q gilt". Laut Satz 3.11 ist dies aber unmöglich. ■

Korollar 4.1
a) HML $\not\leq$ LTL,

b) LTL $\not\leq$ HML.

Beweis (a) Beachte, dass die im Beweis von Satz 4.1, Teil (a), benutzte CTL-Formel bereits in HML ausdrückbar ist.
(b) Folgt trivialerweise aus HML $\leq$ CTL (Satz 3.1). ■

Satz 4.2
Über totalen, linearen und knotenbeschrifteten Transitionssystemen gilt: CTL $\equiv$ LTL.

Beweis ($\geq$) Sei $\varphi \in$ LTL. Wir konstruieren eine CTL-Formel φ' dadurch, dass wir jeden temporalen Operator $\mathtt{X}$, $\mathtt{U}$ oder $\mathtt{R}$ in φ durch $\mathtt{EX}$, $\mathtt{EU}$ bzw. $\mathtt{ER}$ ersetzen. Da auf linearen, totalen Modellen für alle Läufe $\pi = s \ldots$ und alle LTL-Formeln ψ gilt: $\pi \models \psi$ gdw. $s \models \mathtt{E}\psi$, erhalten wir somit, dass φ und φ' auf der Klasse dieser Modelle äquivalent sind.
($\leq$) Sei $\varphi' \in$ CTL. Konstruiere eine LTL-Formel φ aus φ' durch simples Löschen aller Laufquantoren $\mathtt{E}$ und $\mathtt{A}$. Da auf solchen Modellen ein Zustand s eindeutig einen Lauf $\pi = s \ldots$ identifiziert, gilt für alle LTL-Formeln, deren top-level Operator $\mathtt{X}$, $\mathtt{U}$ oder $\mathtt{R}$ ist: $s \models \mathtt{E}\psi$ gdw. $s \models \mathtt{A}\psi$ gdw. $\pi \models \psi$. Für atomare Propositionen gilt dies sowieso, und für boolesche Formeln folgt es somit sofort aus diesen Äquivalenzen. Somit gilt wiederum, dass φ' und φ über linearen und totalen Modellen äquivalent sind. ■

Wir bezeichnen einen Lauf $\pi = s_0 s_1 \ldots$ eines Transitionssystems als *endlich repräsentiert*, wenn es $n, k \in \mathbb{N}$ gibt, so dass für alle $i \geq n$ gilt: $s_{i+k} = s_i$.

Korollar 4.2
Das Problem, zu einem gegebenen Lauf π mit endlicher Repräsentation und einer LTL-Formel φ zu entscheiden, ob $\pi \models \varphi$ gilt, ist in P.

Beweis Dies folgt aus Satz 3.3, welcher besagt, dass das Model Checking Problem für CTL auf beliebigen, endlichen Transitionssystemen in P ist. Außerdem ist die Übersetzung von LTL nach CTL im Beweis von Satz 4.2 linear. ■

Es folgt sogar, dass besagtes Problem in linearer Zeit lösbar ist. Eine entsprechende untere Schranke – d.h. P-Härte – können wir nicht angeben. Es ist noch nicht einmal bekannt, ob das Model Checking Problem für (bestimmte Erweiterungen von) LTL und einem Lauf hart für die Komplexitätsklasse LOGSPACE ist.

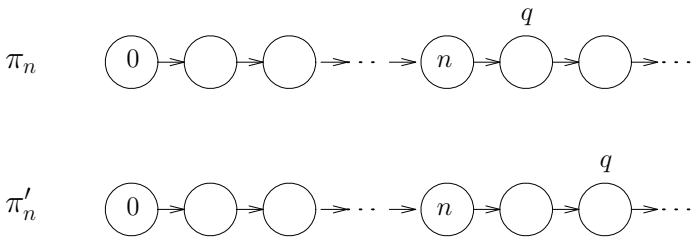
Zum Schluss dieses Abschnitts beweisen wir noch ein explizites Nichtausdrücksbarkeitsresultat.

Definition 4.5
Die *temporale Tiefe* einer LTL-Formel φ ist wie üblich definiert.

$$\begin{aligned} td(q) &:= 0 \\ td(\varphi \vee \psi) &:= \max\{td(\varphi), td(\psi)\} \\ td(\neg\varphi) &:= td(\varphi) \\ td(\mathtt{X}\varphi) &:= 1 + td(\varphi) \\ td(\varphi \mathtt{U} \psi) &:= 1 + \max\{td(\varphi), td(\psi)\} \\ td(\varphi \mathtt{R} \psi) &:= 1 + \max\{td(\varphi), td(\psi)\} \end{aligned}$$

Satz 4.3
Es gibt keine LTL-Formel, die "q gilt nach einer geraden Anzahl von Schritten" ausdrückt.

Beweis Sei $\Pi = \{\pi \mid \pi \text{ ist ein Lauf } s_0 s_1 \ldots \text{ so dass es ein gerades } k \text{ gibt mit } q \in \lambda(s_k)\}$. Wir betrachten die folgenden zwei Familien von Läufen π_n, π'_n für alle $n \in \mathbb{N}$.



Offensichtlich gilt für alle $n \in \mathbb{N}$ entweder $\pi_n \in \Pi$ oder $\pi'_n \in \Pi$, aber nicht beides. Wir zeigen jetzt, dass es keine LTL-Formel gibt, die alle π_n und π'_n unterscheidet.

Zuerst machen wir folgende zwei Beobachtungen über Suffixe dieser beiden Läufe:

1. $\pi_n^{(1)}$ und π_{n-1} sind isomorph, genauso wie $\pi_n'^{(1)}$ und π'_{n-1},
2. π_n und π'_{n-1} sind isomorph.

Beachte, dass keine LTL-Formel isomorphe Läufe unterscheiden kann. Dies folgt aus Lemma 1.3 und Satz 4.2.

Wir zeigen nun durch Induktion über den Formelaufbau für alle $n \in \mathbb{N}$ und alle $\varphi \in$ LTL: wenn $td(\varphi) \leq n$, dann gilt $\pi_n \models \varphi$ gdw. $\pi'_n \models \varphi$. Für atomare Propositionen ist dies offensichtlich, da sich π_n und π'_n nicht in der Beschriftung ihres ersten Zustands unterscheiden für alle $n \in \mathbb{N}$. Für Disjunktionen und Negationen folgt die Behauptung sofort aus der Induktionshypothese.

Sei nun $\varphi = \mathtt{X}\psi$. Es gilt $\pi_n \models \varphi$ gdw. $\pi_n^{(1)} \models \psi$ gdw. (nach Beobachtung 1) $\pi_{n-1} \models \psi$ gdw. (nach der Induktionshypothese) $\pi'_{n-1} \models \psi$ gdw. (nach Beobachtung 1) $\pi_n'^{(1)} \models \psi$ gdw. $\pi'_n \models \varphi$.

Sei nun $\varphi = \psi_1 \mathtt{U} \psi_2$, und es gelte $\pi_n \models \varphi$. Dann gibt es ein $k \in \mathbb{N}$, so dass $\pi_n^{(k)} \models \psi_2$ und für alle $j < k$ gilt $\pi_n^{(j)} \models \psi_1$. Wir unterscheiden zwei Fälle.

Fall 1, $k = 0$. Dann folgt sofort aus der Induktionshypothese für ψ_2, dass auch $\pi'_n \models \psi_2$ gilt, womit auch $\pi'_n \models \varphi$ gezeigt ist.

Fall 2, $k > 0$. Durch Anwendung der Beobachtung zwei für ψ_2 erhalten wir $\pi_n'^{(k+1)} \models \psi_2$ und durch Anwenden dieser Beobachtung für ψ_1 erhalten wir genauso $\pi_n'^{(j+1)} \models \psi_1$ für alle $j = 0, \ldots, k-1$. Beachte, dass $\pi_n^{(0)} \models \psi_1$ gilt. Jetzt wenden wir nur noch die Induktionshypothese für ψ_1 an und erhalten $\pi_n'^{(0)} \models \psi_1$. Zusammen ergibt sich dann $\pi'_n \models \varphi$.

Die Rückrichtung wird analog gezeigt. Hier muss evtl. mit der Beobachtung 2 die Erfülltheit einer Formel in einem $\pi_n'^{(i)}$ auf ein $\pi_n^{(i-1)}$ zurückgeführt werden.

Der Beweis wird dann in der üblichen Weise abgeschlossen. Angenommen, es gäbe ein $\varphi \in$ LTL mit der gewünschten Eigenschaft. Sei $n := td(\varphi)$. Dann würde einerseits $\pi_n \models \varphi$ gdw. $\pi'_n \not\models \varphi$ gelten, aber soeben wurde bewiesen, dass dann auch $\pi_n \models \varphi$ gdw. $\pi'_n \models \varphi$ gelten müsste. ∎

4.5 Entscheidungsverfahren und Komplexität

4.5.1 Das Erfüllbarkeitsproblem

Satz 4.4
Das Erfüllbarkeitsproblem für LTL ist PSPACE-hart.

Beweis Wir skizzieren lediglich den Beweis, da dieser im wesentlichen analog zum Beweis der EXPTIME-Härte von CTL geführt wird (Satz 3.9).

Sei $\mathcal{M} = (Q, \Sigma, \Gamma, q_0, \delta, q_{acc}, q_{rej})$ eine *deterministische* Turing-Maschine, deren Platzbedarf durch ein Polynom $p(n)$ beschränkt ist. Eine Konfiguration von $\mathcal{M}$ in der Berechnung auf einem Eingabewort w repräsentieren wir wieder als ein endliches, lineares Transitionssystem wie im Beweis von Satz 3.9. Da $\mathcal{M}$ deterministisch ist, kann ihre Berechnung auf w durch einen unendlichen Lauf repräsentiert werden.

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

$$(\mathtt{U})\ \frac{\psi \vee (\varphi \wedge \mathtt{X}(\varphi \mathtt{U} \psi)), \Phi}{\varphi \mathtt{U} \psi, \Phi} \qquad (\mathtt{R})\ \frac{\psi \wedge (\varphi \vee \mathtt{X}(\varphi \mathtt{R} \psi)), \Phi}{\varphi \mathtt{R} \psi, \Phi}$$

$$(\mathtt{X})\ \frac{\varphi_1, \ldots, \varphi_n}{\mathtt{X}\varphi_1, \ldots, \mathtt{X}\varphi_n, l_1, \ldots, l_k}\ \text{falls } l_1, \ldots, l_k \text{ konsistent}$$

Abbildung 4.1: Die Erfüllbarkeitstableaux-Regeln für LTL.

Beachte, dass hier die Transitionsrelation δ eine Funktion vom Typ $Q \times \Gamma \to Q \times \Gamma \times \{-1, 0, 1\}$ ist. Es ist daher hier noch nicht einmal nötig, die zu Beginn des Beweis von Satz 3.9 gemachte Einschränkung an Turing Maschinen zu fordern, dass $\mathcal{M}$ in einem Schritt entweder verzweigt oder den Kopf bewegt.

Wiederum gilt, dass die entsprechend konstruierte LTL-Formel $\varphi_{\mathcal{M},w}$ erstens erfüllbar ist, gdw. $w \in L(\mathcal{M})$ ist, und zweitens nur polynomiell groß in $|\mathcal{M}|$ und $|w|$ ist. ∎

Satz 4.5
Das Erfüllbarkeitsproblem für LTL ist in PSPACE.

Korollar 4.3
Das Erfüllbarkeitsproblem für LTL ist PSPACE-vollständig.

Wie im Beweis von Satz 3.7 (endliche Modelleigenschaft für CTL) kann man auch aus einem Erfüllbarkeitstableau für eine LTL-Formel ein endliches Modell für diese Formel bauen. Beachte, dass solch ein Tableau nur einen einzigen Pfad hat, weswegen das konstruierte Modell aus einem einzigen Lauf besteht.

Korollar 4.4
LTL hat die endliche Modelleigenschaft.

Eine weitere Analyse dieser Konstruktion zeigt auch, dass die Größe eines solchen Modells durch die Größe der Eingabeformel beschränkt ist. Beachte, dass jeder Tableau-Pfad der Länge mindestens $|\varphi| \cdot 2^{|\varphi|}$ für eine LTL-Formel φ bereits einen Knoten enthält, welcher zu einem Blatt gemacht werden kann. Dies liefert die kleine Modelleigenschaft entsprechender Größe für LTL.

Korollar 4.5
Für alle LTL-Formeln φ gilt: Wenn φ erfüllbar ist, dann gibt es einen Lauf π, so dass $\pi \models \varphi$ gilt, und π durch höchstens $|\varphi| \cdot 2^{|\varphi|}$ viele Zustände endlich repräsentiert ist.

4.5.2 Das Model Checking Problem

Korollar 4.6
Das Allgemeingültigkeitsproblem für LTL ist PSPACE-vollständig.

Beweis Dies folgt sofort aus Korollar 4.3 und der Tatsache, dass eine LTL-Formel φ erfüllbar ist gdw. $\neg\varphi$ nicht allgemeingültig ist, sowie der Tatsache, dass PSPACE unter Komplement abgeschlossen ist. ∎

Definition 4.6
Sei $\mathcal{P}$ eine endliche Menge von Propositionen. Das *universelle Transitionssystem* $\mathcal{T}_\mathcal{P}$ ist definiert als $(\mathcal{S}, \rightarrow, \lambda)$ mit

- $\mathcal{S} = \{s\} \cup 2^\mathcal{P}$,
- $s \rightarrow P$ und $P' \rightarrow P$ für alle $P, P' \subseteq \mathcal{P}$,
- $\lambda(s) = \emptyset$ und $\lambda(P) = P$ für alle $P \subseteq \mathcal{P}$.

Lemma 4.6
Sei $\varphi \in$ LTL und $\mathcal{P}$ die Menge aller Propositionen, die in φ vorkommen. Dann gilt: $\mathcal{T}_\mathcal{P}, s \models \mathtt{X}\varphi$ gdw. $\models \varphi$.

Beweis Beachte, dass $\mathcal{T}_\mathcal{P}$ so gewählt wurde, dass es zu jeder beliebigen Sequenz $P_1, P_2, \ldots$ mit $P_i \subseteq \mathcal{P}$ für alle $i \in \mathbb{N}$ den Lauf $s, P_1, P_2, \ldots$ in $\mathcal{T}_\mathcal{P}$ gibt.

($\Leftarrow$) Angenommen, es gelte nun $\models \varphi$, d.h. für alle Läufe π eines beliebigen Transitionssystems gilt: $\pi \models \varphi$. Insbesondere gilt dies auch für jeden Lauf $P_1P_2\ldots$ in $\mathcal{T}_\mathcal{P}$. Dann gilt aber auch $s \models \mathtt{X}\varphi$.

($\Rightarrow$) Angenommen, es gilt $\not\models \varphi$, d.h. es gibt ein Transitionssystem $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ und einen Lauf π darin, so dass $\mathcal{T}, \pi \not\models \varphi$, bzw. $\mathcal{T}, \pi \models \neg\varphi$ gilt. Sei $\pi = s_0 s_1 \ldots$. Definiere einen Lauf $\pi' = t_0 t_1 \ldots$ in $\mathcal{T}_\mathcal{P}$ durch $t_i := \lambda(s_i) \cap \mathcal{P}$. Man zeigt leicht durch Induktion über den Formelaufbau, dass π und π' nicht von einer LTL-Formel über der Menge $\mathcal{P}$ von Propositionen unterschieden werden können. Somit gilt insbesondere $\pi' \models \neg\varphi$ und daher $s\pi' \not\models \mathtt{X}\varphi$, weswegen $\mathcal{T}_\mathcal{P}, s \not\models \mathtt{X}\varphi$ gilt. ∎

Satz 4.6
Das Problem, zu einem gegebenen Zustand s eines Transitionssystems $\mathcal{T}$ und einer LTL-Formel φ zu entscheiden, ob $\mathcal{T}, s \models \varphi$ gilt, ist PSPACE-hart.

Beweis Laut Korollar 4.6 ist das Allgemeingültigkeitsproblem für LTL PSPACE-hart. Lemma 4.6 beschreibt eine Reduktion des Allgemeingültigkeitsproblems auf das Model Checking Problem für Zustände. Beachte, dass die Reduktion polynomiell in der Größe der Formel φ für eine feste Menge von Propositionen $\mathcal{P}$ ist. ∎

Dieser Beweis zeigt sogar noch eine Verschärfung des Resultats in Satz 4.6: Es gibt ein Transitionssystem $\mathcal{T}$ und einen Zustand s, so dass das Model Checking Problem auf diesem festen $\mathcal{T}$ und s bereits PSPACE-hart ist – sprich die Ausdruckskomplexität von LTL ist bereits PSPACE-hart.

$$(\vee)\ \frac{s \vdash \psi_0, \psi_1, \Phi}{s \vdash \psi_0 \vee \psi_1, \Phi} \qquad (\wedge)\ \frac{s \vdash \psi_0, \Phi \qquad s \vdash \psi_1, \Phi}{s \vdash \psi_0 \wedge \psi_1, \Phi}$$

$$(\mathtt{U})\ \frac{s \vdash \psi \vee (\varphi \wedge \mathtt{X}(\varphi \mathtt{U} \psi)), \Phi}{s \vdash \varphi \mathtt{U} \psi, \Phi} \qquad (\mathtt{R})\ \frac{s \vdash \psi \wedge (\varphi \vee \mathtt{X}(\varphi \mathtt{R} \psi)), \Phi}{s \vdash \varphi \mathtt{R} \psi, \Phi}$$

$$(\mathtt{X})\ \frac{t_1 \vdash \varphi_1, \ldots, \varphi_n \quad \ldots \quad t_n \vdash \varphi_1, \ldots, \varphi_n}{s \vdash \mathtt{X}\varphi_1, \ldots, \mathtt{X}\varphi_n, l_1, \ldots, l_k} \text{ falls } \{t_1, \ldots, t_n\} = \{t \mid s \to t\}$$

Abbildung 4.2: Die Model-Checking-Tableau-Regeln für LTL.

Satz 4.7
Das Problem, zu einem gegebenen Zustand s eines Transitionssystems $\mathcal{T}$ und einer LTL-Formel φ zu entscheiden, ob $\mathcal{T}, s \models \varphi$ gilt, ist in PSPACE.

Beweis Per Reduktion auf das Allgemeingültigkeitsproblem. (Übung) ∎

Im Gegensatz zur Ausdruckskomplexität ist die Datenkomplexität von LTL einfach.

Korollar 4.7
Das Problem, zu einer festen LTL-Formel φ zu entscheiden, ob für ein gegebenes Transitionssystem $\mathcal{T}$ mit Zustand s gilt $\mathcal{T}, s \models \varphi$, ist in NLOGSPACE.

4.6 Unäres LTL

Wie in Abschnitt 3.5 bei CTL betrachten wir auch wieder Fragmente von LTL, die durch Einschränkung der temporalen Operatoren oder deren Gebrauch entstehen.

Definition 4.7
Formeln der Logik LTL$^-$ über einer Menge $\mathcal{P}$ von Propositionen sind gegeben durch folgende Grammatik.

$$\varphi \ ::= \ q \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \neg\varphi \mid \mathtt{X}\varphi \mid \mathtt{F}\varphi \mid \mathtt{G}\varphi$$

wobei $q \in \mathcal{P}$. Die Semantik ergibt sich wiederum eindeutig aus der Semantik der Superlogik LTL.

Satz 4.8
Das Erfüllbarkeitsproblem für LTL$^-$ ist PSPACE-vollständig.

Beweis Die obere Schranke wird trivialerweise von LTL (Satz 4.5) geerbt. Für die untere Schranke vergewissert man sich wie im Beweis von Satz 3.13, dass die Reduktion vom Wortproblem für deterministische, polynomiell platzbeschränkte Turing Maschinen konstruierten LTL-Formeln nicht den U- oder R-Operator verwendt. ∎

Korollar 4.8
Das Model Checking Problem für LTL^- und Zustände ist PSPACE-vollständig.

Beweis Die obere Schranke wird wiederum trivialerweise von LTL geerbt, die untere Schranke folgt aus Satz 4.8 mittels einer Reduktion über das Allgemeingültigkeitsproblem für LTL^- und dem universellen Transitionssystem $\mathcal{T}_\mathcal{P}$ wie in Satz 4.6. ■

Korollar 4.9
$\mathrm{LTL}^- \lneq \mathrm{LTL}$.

Beweis Die Inklusion ist natürlich trivial. Die Striktheit folgt aus Satz 3.16, in dem die beiden Logiken UCTL und CTL bzgl. Ausdruckstärke getrennt werden. Die dazu konstruierten Transitionssysteme, die von keiner UCTL-, jedoch von einer CTL-Formel unterschieden werden, bestehen nur aus einem einzigen Lauf. Daher überträgt sich dieses Resultat direkt auf die Linearzeitlogiken LTL^- und LTL. ■

4.7 Stutter-Invariant LTL

Definition 4.8
Zwei Läufe $\pi = s_0 s_1 \ldots$ und $\pi' = t_0 t_1 \ldots$ heißen *stutter-äquivalent*, falls es zwei Sequenzen von Indizes $i_0 < i_1 < i_2 < \ldots$ und $j_0 < j_1 < j_2 < \ldots$ gibt mit $i_0 = 0 = j_0$, so dass für alle $k \geq 0$ gilt:

$$\lambda(s_{i_k}) = \lambda(s_{i_k+1}) = \ldots = \lambda(s_{i_{k+1}-1}) = \lambda(t_{j_k}) = \lambda(t_{j_k+1}) = \ldots = \lambda(t_{j_{k+1}-1})$$

wobei λ die übliche Beschriftungsfunktion ist, die einem Zustand eine Menge von Propositionen zuordnet.

Eine Menge Π von Läufen (nicht notwendigerweise eines Transitionssystems) heißt *stutter-invariant*, wenn für alle stutter-äquivalenten π, π' gilt: $\pi \in \Pi$ gdw. $\pi' \in \Pi$.

Beispiel 4.4
Betrachte die zwei eindeutigen Läufe, die jeweils in den linken Zuständen der beiden folgenden Transitionssysteme starten.

Diese sind stutter-äquivalent, was durch die beiden Sequenzen von Indizes $0, 1, 2, \ldots$ und $0, 2, 3, 5, 6, 8, 9, \ldots$ bezeugt wird.

Definition 4.9
Das stutter-invariante Fragment von LTL entsteht durch Weglassen des temporalen `X`-Operators. Formeln der Logik $\mathrm{LTL}^{\mathsf{si}}$ über einer Menge $\mathcal{P}$ von Propositionen sind gegeben durch die folgende Grammatik.

$$\varphi \ ::= \ q \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \neg\varphi \mid \varphi \mathtt{U} \varphi \mid \varphi \mathtt{R} \varphi$$

wobei $q \in \mathcal{P}$. Die Semantik ist wiederum eindeutig durch die Superlogik LTL festgelegt.

Der Name dieses Fragments von LTL kommt daher, dass LTL ohne den X-Operator nur stutter-invariante Eigenschaften beschreiben kann.

Lemma 4.7
Für alle $\varphi \in \text{LTL}^{\mathsf{si}}$ gilt: $[\![\varphi]\!]$ ist stutter-invariant.

Beweis Übung. ■

Korollar 4.10
$\text{LTL}^{\mathsf{si}} \lneq \text{LTL}$.

Beweis Die Inklusion ist trivial. Die Striktheit folgt aus Lemma 4.7, da es offensichtlich LTL-Formeln gibt, deren Semantik keine stutter-invariante Menge von Läufen ist, z.B. $q \wedge \mathtt{X}\neg q$. ■

Definition 4.10
Ein Lauf $\pi = s_0 s_1 \ldots$ mit Beschriftungsfunktion λ heißt *stutter-frei*, wenn eine der beiden folgenden Bedingungen zutrifft.

1. Für alle $i \in \mathbb{N}$ ist $\lambda(s_i) \neq \lambda(s_{i+1})$.
2. Es gibt ein $k \in \mathbb{N}$, so dass $\lambda(s_i) \neq \lambda(s_{i+1})$ für alle $i < k$ und $\lambda(s_i) = \lambda(s_{i+1})$ für alle $i \geq k$ gilt.

Lemma 4.8
Jeder Lauf π is stutter-äquivalent zu einem stutter-freien π'.

Beweis Übung. ■

Lemma 4.9
Sei Π eine stutter-invariante Menge von Läufen und $\varphi \in \text{LTL}^{\mathsf{si}}$, so dass für alle stutter-freien Läufe π gilt: $\pi \models \varphi$ gdw. $\pi \in \Pi$. Dann ist $\Pi = [\![\varphi]\!]$.

Beweis Angenommen, $\Pi \neq [\![\varphi]\!]$. Da LTL^{si} unter Komplement abgeschlossen ist, können wir davon ausgehen, dass es ein $\pi' \in \Pi$ gibt, so dass $\pi' \notin [\![\varphi]\!]$. Nach Lemma 4.8 existiert aber ein stutter-freies π, und nach Voraussetzung gilt auch $\pi \in \Pi$. Aufgrund von Lemma 4.7 kann φ aber nicht zwischen π und π' unterscheiden, also gilt $\pi' \not\models \varphi$. Dies widerspricht aber der Annahme, dass $\pi \models \varphi$ gdw. $\pi \in \Pi$. ■

Satz 4.9
Eine stutter-invariante Menge Π von Läufen ist in LTL definierbar gdw. sie in LTL^{si} definierbar ist.

Beweis ($\Leftarrow$) Angenommen, es gibt eine LTL^{si}-Formel φ, so dass $\Pi = [\![\varphi]\!]$. Da LTL^{si} ein Fragment von LTL ist, ist Π somit offensichtlich in LTL definierbar. Darüberhinaus zeigt Lemma 4.7 auch noch, dass Π stutter-invariant ist.

($\Rightarrow$) Angenommen, Π ist stutter-invariant und es gibt eine LTL-Formel φ, so dass $\Pi = [\![\varphi]\!]$. Sei $\mathcal{P} := \{q_1, \ldots, q_k\}$ die Menge alle Propositionen, die in φ vorkommen.

Wir konstruieren nun durch Induktion über den Formelaufbau eine LTL$^{\mathsf{si}}$-Formel $si(\varphi)$, so dass $[\![si(\varphi)]\!] = \Pi$ gilt. Laut Lemma 4.9 reicht es aus zu zeigen, dass φ und $si(\varphi)$ stutter-freie Läufe nicht unterscheiden können.

Fall $\varphi = q$. Setze $si(q) := q$. Die Behauptung gilt dann trivialerweise.

Fall $\varphi = \psi_1 \vee \psi_2$. Setze $si(\psi_1 \vee \psi_2) := si(\psi_1) \vee si(\psi_2)$. Die Behauptung folgt sofort aus der Induktionshypothese. Dasselbe gilt für die Fälle $\varphi = \neg\psi$ mit $si(\neg\psi) := \neg si(\psi)$ und $\varphi = \psi_1 \mathtt{U} \psi_2$ mit $si(\psi_1 \mathtt{U} \psi_2) := si(\psi_1) \mathtt{U} si(\psi_2)$.

Es bleibt lediglich der Fall $\varphi = \mathtt{X}\psi$ übrig. Dieser ist offensichtlich schwieriger, da die zu konstruierende LTL$^{\mathsf{si}}$-Formel den X-Operator nicht mehr enthalten darf. Nach Def. 4.10 reicht es aus zu sagen, dass entweder

- alle Propositionen, die jetzt (nicht) gelten, immer (nicht) gelten, und ψ jetzt gilt, oder
- es eine Proposition gibt, in deren Wert sich der jetzige und der nachfolgende Zustand unterscheiden, und ψ gilt, wenn diese Proposition ihren neuen Wert annimmt; gleichzeitig verändert keine andere Proposition dazwischen ihren Wert.

Wir setzen

$$\begin{aligned} si(\mathtt{X}\psi) \;:=\; & \Big(si(\psi) \;\wedge\; \bigwedge_{i=1}^{k} (q_i \wedge \mathtt{G}q_i) \vee (\neg q_i \wedge \mathtt{G}\neg q_i) \Big) \\ & \vee \Big(\bigvee_{i=1}^{k} (q_i \mathtt{U} (\neg q_i \wedge si(\psi)) \;\wedge\; \bigwedge_{j \neq i} (q_j \mathtt{U} \neg q_i \;\vee\; \neg q_j \mathtt{U} \neg q_i) \\ & \qquad \vee (\neg q_i \mathtt{U} (q_i \wedge si(\psi)) \;\wedge\; \bigwedge_{j \neq i} (q_j \mathtt{U} q_i \;\vee\; \neg q_j \mathtt{U} q_i) \Big) \end{aligned}$$

Somit gilt $\pi \models \mathtt{X}\psi$ gdw. $\pi \models si(\mathtt{X}\psi)$ für alle stutter-freien Läufe $\pi = s_0 s_1 \ldots$ gilt. Man beachte, dass ein Suffix eines stutter-freien Laufes wiederum stutter-frei ist, weswegen die Induktionshypothese überhaupt anwendbar ist. ■

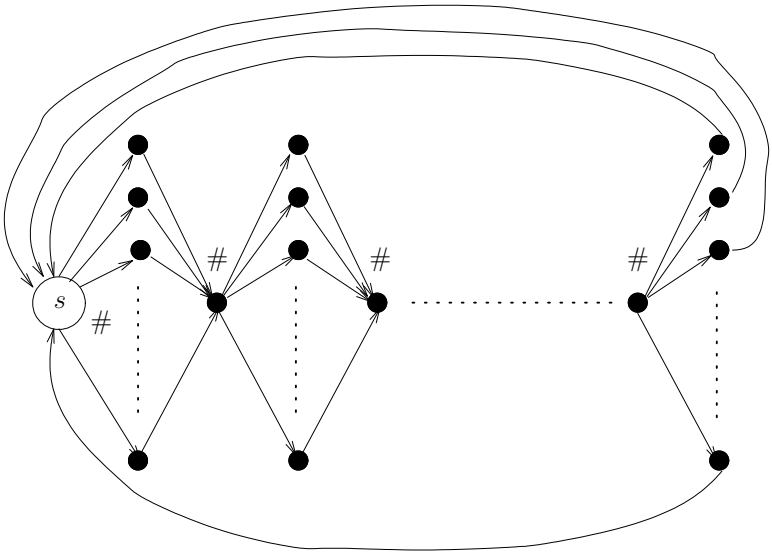
Korollar 4.11
Eine stutter-invariante Menge von Läufen, die von einer LTL-Formel φ definiert wird, wird auch von einer LTL$^{\mathsf{si}}$-Formel φ' definiert, so dass $|\varphi'| = O(|\varphi|^3)$ gilt.

PSPACE ist natürlich eine obere Schranke an das Model Checking Problem für LTL$^{\mathsf{si}}$. Eine entsprechende untere Schranke wird nicht von LTL geerbt. Beachte, dass bei LTL PSPACE-Härte für das Model Checking Problem über den Umweg Allgemeingültigkeitsproblem auf das Erfüllbarkeitsproblem reduziert wurde. Der Beweis der PSPACE-Härte dessen macht jedoch von dem X-Operator Gebrauch, weswegen die Behauptung nicht sofort aus früheren Resultaten folgt.

Satz 4.10
Das Model Checking Problem für LTL$^{\mathsf{si}}$ ist PSPACE-hart.

Beweis Sei $\mathcal{M} = (Q, \Sigma, \Gamma, q_0, \delta, q_{acc}, q_{rej})$ eine deterministische Turing Maschine, deren Platzbedarf durch ein Polynom $p(n)$ beschränkt ist. Sei $w = a_1 \dots a_n \in \Sigma^*$ eine Eingabe an $\mathcal{M}$. Wir konstruieren ein Transitionssystem $\mathcal{T}_{\mathcal{M},w}$ mit Zustand s und eine LTL$^{\mathsf{si}}$-Formel $\varphi_{\mathcal{M},w}$, so dass gilt: $w \notin L(\mathcal{M})$ gdw. $s \not\models \neg\varphi_{\mathcal{M},w}$. Da PSPACE unter Komplement abgeschlossen ist, folgt das Härteresult, solange die Reduktion polynomiell ist.

Die Menge der atomaren Propositionen, über denen $\mathcal{T}_{\mathcal{M},w}$ und $\varphi_{\mathcal{M},w}$ definiert sind, ist $\mathcal{P} := \Gamma \cup Q \times \Gamma \cup \{\#\}$. $\mathcal{T}_{\mathcal{M},w}$ besteht aus $p(n) \cdot (1 + |\Gamma| \cdot (|Q| + 1))$ vielen Zuständen, die wie folgt angeordnet sind.



Dabei gibt es in jedem diamant-artigen Teil für jedes $x \in \Gamma \cup Q \times \Gamma$ genau einen Zustand, dessen Beschriftung $\{x\}$ ist.

Wir skizzieren zunächst unter Zuhilfenahme des X-Operators eine LTL-Formel $\varphi'_{\mathcal{M},w}$, so dass ein Lauf π – beginnend in s – ein Modell von $\varphi'_{\mathcal{M},w}$ ist, gdw. π eine nicht-akzeptierende Berechnung von $\mathcal{M}$ auf w in der folgenden Weise kodiert. Eine Konfiguration $b_1 \dots b_{k-1} q b_k \dots b_{p(n)}$ wird modelliert durch einen Pfad mit Beschriftung $\#b_1\# \dots \#b_{k-1}\#(q, b_k)\# \dots \#b_{p(n)}$. Solche Teilstücke werden sukzessive zu einem Lauf konkateniert.

Die Formel $\varphi'_{\mathcal{M},w}$ besteht wie im Beweis von Satz 3.9 aus Konjunkten, welche besagen, dass jedes Teilstück eine legale Konfiguration ist, dass das erste Teilstück die Anfangskonfiguration darstellt, sich aufeinanderfolgende Teilstücke gemäß der Transitionsrelation δ verhalten und irgendwann einmal ein Zustand mit Beschriftung (q_{rej}, b) für ein $b \in \Gamma$ erreicht wird.

Beachte nun, dass für jeden Lauf π, beginnend irgendwo in $\mathcal{T}_{\mathcal{M},w}$, und jede LTL-Formel ψ gilt:

$$\pi \models \mathtt{X}\psi \quad \text{gdw.} \quad \pi \models \#\mathtt{U}(\neg\# \wedge \psi) \vee \neg\#\mathtt{U}(\# \wedge \psi)$$

Somit läßt sich $\varphi'_{\mathcal{M},w}$ in eine LTL$^{\mathsf{si}}$-Formel $\varphi_{\mathcal{M},w}$ transformieren, so dass gilt: $w \notin L(\mathcal{A})$ gdw. $s \not\models \neg\varphi_{\mathcal{M},w}$. Dies folgt u.a. auch direkt aus Satz 4.9, da leicht zu sehen ist, dass jeder Lauf in $\mathcal{T}_{\mathcal{M},w}$ stutter-frei ist.

Beachte, dass $\neg\varphi_{\mathcal{M},w}$ wiederum exponentiell länger als $\varphi'_{\mathcal{M},w}$ sein kann, aber die Anzahl ihrer Unterformeln nur konstant größer ist. ∎

Korollar 4.12
Das Model Checking Problem für LTL$^{\mathsf{si}}$ ist PSPACE-vollständig.

Es bleibt die Frage nach dem Erfüllbarkeitsproblem für LTL$^{\mathsf{si}}$ zu klären. Wiederum ist dies trivialerweise in PSPACE, da das Erfüllbarkeitsproblem für LTL in PSPACE ist. Wir zeigen eine entsprechende untere Schranke durch Reduktion auf das Model Checking Problem. Beachte, dass bei LTL dies umgekehrt gezeigt wurde.

Satz 4.11
Das Erfüllbarkeitsproblem für LTL$^{\mathsf{si}}$ ist PSPACE-hart.

Beweis Sei $\mathcal{T} = (\mathcal{S}, \to, \lambda)$ ein endliches Transitionssystem über einer Menge $\mathcal{P}$ von Propositionen mit $\mathcal{S} \cap \mathcal{P} = \emptyset$, $s \in \mathcal{S}$ und $\varphi \in \text{LTL}^{\mathsf{si}}$. Wir konstruieren eine Formel $\psi_{\mathcal{T},s,\varphi}$, die erfüllbar ist, gdw. $\mathcal{T}, s \not\models \varphi$. Wegen dem Komplementabschluss von PSPACE reicht dies aus.

Zuerst müssen wir $\mathcal{T}$ geeignet axiomatisieren. Sei $\mathcal{P}' := \mathcal{P} \cup \mathcal{S}$. Für jeden Zustand s definiere

$$\begin{aligned}
\alpha_s &:= \bigwedge_{q \in \lambda(s)} q \ \wedge \bigwedge_{q \notin \lambda(s)} \neg q \\
\beta_s &:= \bigvee_{s \to t} t \\
\chi_s &:= s \ \to \ \alpha_s \wedge \begin{cases} \mathtt{G}\alpha_s \ \vee \ \alpha_s \mathtt{U}(\neg s \wedge \beta_s) \ , & \text{falls } s \to s \\ s \mathtt{U} \beta_s \ , & \text{sonst} \end{cases}
\end{aligned}$$

Setze dann

$$\psi_{\mathcal{T},s,\varphi} := s \ \wedge \ \mathtt{G}\Big(\bigvee_{t \in \mathcal{S}} t \ \wedge \bigwedge_{t,t' \in \mathcal{S}, t \neq t'} \neg(t \wedge t') \wedge \bigwedge_{t \in \mathcal{S}} \chi_t \Big) \ \wedge \ \neg\varphi$$

Dann gilt: Ein Lauf, der die ersten beiden Konjunkte erfüllt, ist stutter-äquivalent zu einem Lauf in $\mathcal{T}$, der in s beginnt. Somit ist $\psi_{\mathcal{T},s,\varphi}$ erfüllbar, gdw. $s \not\models \varphi$. ∎

Korollar 4.13
Das Erfüllbarkeitsproblem und das Allgemeingültigkeitsproblem für LTL$^{\mathsf{si}}$ ist PSPACE-vollständig.

4.8 Minimal LTL

In diesem Abschnitt kombinieren wir die Restriktionen aus den vorherigen beiden Abschnitten.

Definition 4.11
Formel der Logik *Minimal LTL* ($\text{LTL}^{\mathsf{min}}$) über einer Menge $\mathcal{P}$ von Propositionen sind gegeben durch die folgende Grammatik.

$$\varphi \ ::= \ q \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \neg\varphi \mid \mathtt{F}\varphi \mid \mathtt{G}\varphi$$

wobei $q \in \mathcal{P}$. Die Semantik ergibt sich wiederum eindeutig aus der der Superlogik LTL.

Wir erinnern daran, dass die Restriktionen von LTL auf LTL^{-} und auf LTL^{si} nichts an der Komplexität der Logik ändern. Die Kombination der beiden Restriktionen macht die Logik jedoch einfacher, was folgendes Resultat verdeutlicht.

Satz 4.12
Für alle $\varphi \in \text{LTL}^{\mathsf{min}}$ gilt: Wenn φ erfüllbar ist, dann hat es ein Modell der Größe höchstens $|\varphi|$.

Beweis Angenommen φ ist erfüllbar. O.B.d.A. nehmen wir an, dass φ in positiver Normalform gegeben ist. Wegen Satz 4.5 hat φ ein Modell π mit endlicher Repräsentation. Seien $s_0, \ldots, s_k$ die Zustände in dem Modell, d.h. $\pi = s_0 \ldots s_l \ldots s_k s_l \ldots$ für ein $l \in \{0, \ldots, k\}$. Wir schreiben $i \trianglelefteq j$ für $0 \leq i, j \leq k$, falls

- $i < l$ und $i \leq j$, oder
- $i \geq l$ und $j \geq l$.

Es gilt also $i \trianglelefteq j$, gdw. s_j in π irgendwann nach s_i vorkommt.

Definiere zunächst für alle $i = 0, \ldots, k$: $M_i^\pi := \{\psi \in \mathit{Sub}(\varphi) \mid \pi^{(i)} \models \psi\}$ als die Menge aller Unterformeln von φ, die auf dem i-ten Suffix von π gelten.

Wir bezeichnen ein s_i, $i \in \{0, \ldots, k\}$ als *wichtig*, falls entweder

- $i = 0$, oder
- $i = l$, oder
- es gibt ein j, so dass $\mathtt{F}\psi \in M_j^\pi$ für ein $\psi \in \mathit{Sub}(\varphi)$ und i ist maximal, so dass $\psi \in M_i^\pi$.

Beachte, dass für alle $j = 0, \ldots, k$ und jedes $\psi \in \mathit{Sub}(\varphi)$ gilt: wenn $\mathtt{F}\psi \in M_j^\pi$ dann gibt es ein i, so dass $\psi \in M_i^\pi$.

Betrachte nun den Lauf π' der aus π durch Streichen aller nicht-wichtigen Zustände entsteht. D.h. es gibt $0 = i_0 < i_1 < \ldots < i_m \in \{0, \ldots, k\}$, so dass i_j für alle j wichtig ist, und π' durch $s_{i_0} s_{i_1} \ldots s_{i_m}$ endlich repräsentiert ist. Wir definieren wiederum wie oben $M_{i_j}^{\pi'} := \{\psi \in \mathit{Sub}(\varphi) \mid \pi^{(j)} \models \psi\}$.

Es bleibt zu zeigen, dass auch π' ein Modell von φ ist. Dazu zeigen wir, dass für alle $j = 0, \ldots, m$ gilt: $M_{i_j}^\pi \subseteq M_{i_j}^{\pi'}$. D.h. wir zeigen durch Induktion über den Formelaufbau, dass für alle j gilt: wenn $\psi \in M_{i_j}^\pi$, dann ist auch $\psi \in M_{i_j}^{\pi'}$. Beachte, dass s_0 wichtig ist und dass $\varphi \in M_0^\pi$ ist, weswegen dies $\pi' \models \varphi$ impliziert.

Für Literale ψ gilt die Behauptung, da sich die Beschriftung eines s_{i_j} in π' nicht von der in π' unterscheidet. Für Disjunktionen und Konjunktionen folgt die Behauptung sofort aus der Induktionshypothese.

Sei $\psi = \mathtt{G}\psi'$ und es gelte $\psi \in M^{\pi}_{i_j}$ für ein j. Dann gilt also $\psi' \in M^{\pi}_{i_{j'}}$ für alle $i_{j'}$ mit $i_j \trianglelefteq i_{j'}$, insbesondere für solche $i_{j'}$, so dass $s_{i_{j'}}$ wichtig ist. Nach Induktionshypothese gilt dann $\varphi \in M^{\pi'}_{i_{j'}}$ für alle $i_{j'}$ mit $i_j \trianglelefteq i_{j'}$, so dass $s_{i_{j'}}$ in π' vorkommt. Dann gilt aber auch $\psi \in M^{\pi'}_{i_j}$.

Sei nun $\psi = \mathtt{F}\psi'$ und es gelte $\psi \in M^{\pi}_{i_j}$ für ein j. Aufgrund obiger Bemerkung gibt es dann ein $h \in \{0, \ldots, k\}$, so dass $i_j \trianglelefteq h$ und $\psi' \in M^{\pi}_{h}$. Da es nur endlich viele Kandidaten für solch ein h gibt, gibt es auch ein maximales, und es gilt $h = i_{j'}$ für ein j'. D.h. der Zustand s_h ist ebenfalls wichtig. Nach Voraussetzung gilt dann auch $\psi' \in M^{\pi'}_{i_{j'}}$, und da $i_j \trianglelefteq i_{j'}$ in π', gilt auch $\psi \in M^{\pi'}_{i_j}$.

Somit ist ein potentiell kleineres Modell π' für φ gefunden. Es bleibt zu zeigen, dass die Größe von π' entsprechend beschränkt ist. Da es offensichtlich nur $|\varphi| - 1$ viele Unterformeln der Form $\mathtt{F}\psi$ in $Sub(\varphi)$ geben kann, kann es auch nur höchstens $|\varphi|+1$ viele wichtigen Zustände in π, bzw. allgemeine Zustände in π' geben. Man überlegt sich leicht, dass der Zustand s_l nur als wichtig markiert wurde, damit π' einen unendlichen Lauf bildet. Lässt man auch solche endlichen Repräsentationen von Läufen zu, in denen sich nichts wiederholt – z.B. mit der impliziten Maßgabe, dass der letzte Zustand unendlich oft wiederholt wird, um einen unendlichen Lauf zu erhalten – dann reduziert sich die Anzahl der wichtigen Zustände und damit die Größe von π' auf $|\varphi|$. ∎

Korollar 4.14
Das Erfüllbarkeitsproblem für $\mathrm{LTL}^{\mathsf{min}}$ ist in NP.

Beweis Laut Satz 4.12 ist eine $\mathrm{LTL}^{\mathsf{min}}$-Formel φ erfüllbar gdw. sie ein Modell der Größe höchstens $|\varphi|$ hat. Ein nicht-deterministischer Algorithmus kann in polynomieller Zeit $|\varphi|$ viele Beschriftungen von Zuständen mit den Propositionen, die in φ vorkommen, raten. Laut Korollar 4.2 lässt sich deterministisch in polynomieller Zeit überprüfen, ob der erratene Lauf mit endlicher Repräsentation ein Modell von φ ist. ∎

Korollar 4.15
Das Allgemeingültigkeits- und das Model Checking Problem für $\mathrm{LTL}^{\mathsf{min}}$ sind in co-NP.

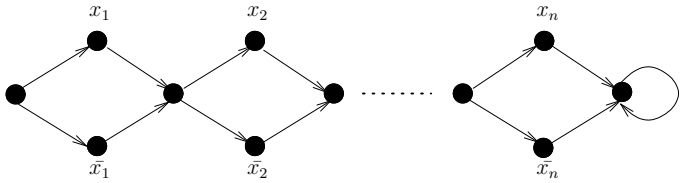
Beweis Dass das Allgemeingültigkeitsproblem in co-NP ist, folgt sofort aus Kor. 4.14 und dem Komplementabschluss von $\mathrm{LTL}^{\mathsf{min}}$. Die obere Schranke überträgt sich auf das Model Checking Problem wie im Beweis von Satz 4.11, wo gezeigt wurde, dass das Model Checking Problem für $\mathrm{LTL}^{\mathsf{si}}$ höchstens so schwer wie das Komplement des Erfüllbarkeitsproblems ist. ∎

Satz 4.13
Das Model Checking Problem für $\mathrm{LTL}^{\mathsf{min}}$ ist co-NP-hart.

Beweis Bekanntermaßen ist KNF-SAT, das Erfüllbarkeitsproblem für aussagenlogische Formeln in konjunktiver Normalform, NP-hart. Somit ist dessen Komplement DNF-VAL – das Allgemeingültigkeitsproblem für aussagenlogische Formeln in disjunktiver Normalform – co-NP-hart. Wir reduzieren das Model Checking Problem für $\mathrm{LTL}^{\mathsf{min}}$ auf dieses.

Sei $\Phi = C_1 \vee \ldots \vee C_m$ eine aussagenlogische Formel über den Variablen $x_1, \ldots, x_n$ und für alle $i = 1, \ldots, m$: $C_i = \bigwedge_{j=1}^{k_i} l_{ij}$ für ein k_i und Literale l_{ij}. Sei $\mathcal{P} := \{x_i, \bar{x_i} \mid i = 1, \ldots, n\}$ die Menge der atomaren Propositionen, über denen Transitionssystem und $\mathrm{LTL}^{\mathsf{min}}$-Formel definiert werden. Intuitiv besagt x_i bzw. $\bar{x_i}$, dass der Wert der Variablen x_i 1 bzw. 0 ist, und c_i, dass ein Literal in der Konjunktion C_i vorkommt.

Das Transitionssystem $\mathcal{T}_\Phi$ ist definiert wie folgt.



Sei s außerdem die Bezeichnung des Zustands ganz links.

Für jedes Literal l_{ij} aus Φ definieren wir eine atomare $\mathrm{LTL}^{\mathsf{min}}$-Formel l'_{ij} in natürlicher Weise: $l'_{ij} := x_h$, falls $l_{ij} = x_h$, und $l'_{ij} := \bar{x_h}$, falls $l_{ij} = \neg x_h$. Definiere nun eine $\mathrm{LTL}^{\mathsf{min}}$-Formel wie folgt.

$$\varphi_\Phi \quad := \quad \bigvee_{i=1}^{m} \bigwedge_{j=1}^{k_i} \mathtt{F} l'_{ij}$$

Beachte, dass jeder Lauf in $\mathcal{T}_\Phi$, der in s beginnt, eindeutig eine Belegung η der Variablen $x_1, \ldots, x_n$ mit Werten 0 oder 1 definiert. Die Variable x_h erhält den Wert 1, falls ein Zustand mit Beschriftung x_h auf dem Lauf vorkommt. Ist dies nicht der Fall, dann kommt ein Zustand mit Beschriftung $\bar{x_h}$ auf dem Lauf vor, und dann erhält sie den Wert 0. Umgekehrt gilt genauso: Jeder der 2^n vielen Variablenbelegungen η entspricht eindeutig ein Lauf π_η in $\mathcal{T}_\Phi$ beginnend in s.

Jetzt gilt: Φ ist wahr unter der Belegung η gdw. es ein $i \in \{1, \ldots, n\}$ gibt, so dass η alle Literale in C_i wahr macht. Dies ist genau dann der Fall, wenn $\pi_\eta \models \varphi_\Phi$ ist. Somit ist Φ allgemeingültig gdw. $\mathcal{T}_\Phi, s \models \varphi_\Phi$. Beachte, dass diese Reduktion in polynomieller Zeit durchführbar ist. ■

Korollar 4.16
Das Erfüllbarkeitsproblem für $\mathrm{LTL}^{\mathsf{min}}$ ist NP-hart.

Beweis Da $\mathrm{LTL}^{\mathsf{min}}$ ein Fragment von $\mathrm{LTL}^{\mathsf{si}}$ ist, überträgt sich die Reduktion des Erfüllbarkeitsproblems von $\mathrm{LTL}^{\mathsf{si}}$ auf das Komplement des Model Checking Problems für $\mathrm{LTL}^{\mathsf{si}}$ aus dem Beweis von Satz 4.11 auf $\mathrm{LTL}^{\mathsf{min}}$. ■

Korollar 4.17
Für $\mathrm{LTL}^{\mathsf{min}}$ ist das Erfüllbarkeitsproblem NP-vollständig, Allgemeingültigkeits- und Model Checking Problem sind jeweils co-NP-vollständig.

4.9 LTL mit Vergangenheitsoperatoren

Bisher haben aller temporalen Operatoren immer nur Aussagen über die Zukunft gemacht. U.U. ist es jedoch auch wünschenswert, Aussagen über die Vergangenheit eines Laufes zu machen, z.B. "immer wenn die Bahnschranke geschlossen wird, wurde dies vorher auch signalisiert".

Definition 4.12
Formeln der Logik PLTL über einer Menge $\mathcal{P}$ von atomaren Propositionen sind gegeben durch die folgende Grammatik.

$$\varphi \;:=\; q \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \neg\varphi \mid \mathtt{X}\varphi \mid \mathtt{Y}\varphi \mid \varphi\mathtt{U}\varphi \mid \varphi\mathtt{R}\varphi \mid \varphi\mathtt{S}\varphi \mid \varphi\mathtt{H}\psi$$

wobei $q \in \mathcal{P}$. Dabei ist `Y` ("yesterday") der entsprechende Vergangenheitsoperator zum Zukunftsoperator `X`, `S` ("since") der entsprechende für `U` und `H` ("has started") der für `R`.

Die Semantik läßt sich nicht ohne weiteres von LTL auf PLTL übertragen, da Läufe einseitig unendliche Objekte sind. Auf solchen Läufen würde z.B. nicht die Äquivalenz $\neg\mathtt{Y}\varphi \equiv \mathtt{Y}\neg\varphi$ gelten. Aus diesem Grund nehmen wir zuerst einmal an, dass ein Lauf ein zweiseitig unendliches Objekt ist. Dann muss die Semantik allerdings leicht anders formuliert werden.

Definition 4.13
Sei $\pi = \ldots s_{-1}s_0s_1\ldots$ ein Lauf mit Beschriftungsfunktion λ. Die Semantik einer PLTL-Formel ist für alle $i \in \mathbb{Z}$ induktiv definiert wie folgt.

$$\begin{aligned}
\pi, i \models q &\quad \text{iff} \quad q \in \lambda(s_i)\\
\pi, i \models \varphi \vee \psi &\quad \text{iff} \quad \pi, i \models \varphi \text{ oder } \pi, i \models \psi\\
\pi, i \models \varphi \wedge \psi &\quad \text{iff} \quad \pi, i \models \varphi \text{ und } \pi, i \models \psi\\
\pi, i \models \neg\varphi &\quad \text{iff} \quad \pi, i \not\models \varphi\\
\pi, i \models \mathtt{X}\varphi &\quad \text{iff} \quad \pi, i+1 \models \varphi\\
\pi, i \models \mathtt{Y}\varphi &\quad \text{iff} \quad \pi, i-1 \models \varphi\\
\pi, i \models \varphi\mathtt{U}\psi &\quad \text{iff} \quad \exists k \geq i,\ \pi, k \models \psi \text{ und } \forall j \text{ mit } i \leq j < k : \pi, j \models \varphi\\
\pi, i \models \varphi\mathtt{R}\psi &\quad \text{iff} \quad \forall k \text{ mit } k \geq i : \pi, k \models \psi \text{ oder } \exists j \text{ mit } i \leq j < k \text{ und } \pi, j \models \varphi\\
\pi, i \models \varphi\mathtt{S}\psi &\quad \text{iff} \quad \exists k \leq i,\ \pi, k \models \psi \text{ und } \forall j \text{ mit } k < j \leq ik : \pi, j \models \varphi\\
\pi, i \models \varphi\mathtt{R}\psi &\quad \text{iff} \quad \forall k \text{ mit } k \leq i : \pi, k \models \psi \text{ oder } \exists j \text{ mit } k < j \leq i \text{ und } \pi, j \models \varphi
\end{aligned}$$

Wir schreiben auch $\pi \models \varphi$, falls $\pi, 0 \models \varphi$, und $[\![\varphi]\!] := \{\pi \mid \pi \models \varphi\}$.

Offensichtlich können wir uns bei PLTL wieder auf Formeln in positiver Normalform beschränken.

Lemma 4.10
Jede PLTL-Formel φ ist äquivalent zu einer PLTL-Formel φ' in der das Negationssymbol nur vor atomaren Propositionen vorkommt, und es gilt $|\varphi'| = O(|\varphi|)$.

Beweis Übung. ∎

Beispiel 4.5
Vergangenheitsoperatoren können für die Spezifikation von Korrektheitsaussagen nützlich sein. So wird z.B. bei der Ampelmodellierung aus Bsp. 4.2 verlangt, dass auf jede atomare Proposition `gedrueckt` irgendwann einmal die Proposition `fgruen` folgt.

$$\mathtt{G}\big(\ \mathtt{gedrueckt} \rightarrow \mathtt{frot}\ \mathtt{U}\ (\mathtt{fgruen} \wedge \neg\mathtt{gedrueckt})\ \big)$$

Umgekehrt möchte man eventuell spezifizieren, dass die Fußgängerampel *nur dann* grün wird, wenn vorher der Signalknopf gedrückt wurde.

$$\mathtt{G}\big(\ \mathtt{fgruen} \rightarrow (\mathtt{Yfrot})\ \mathtt{S}\ \mathtt{gedrueckt}\ \big)$$

Beachte, dass sich letztere Formel auch in LTL ausdrücken läßt, solange diese nur auf einseitig unendlichen Pfaden interpretiert wird.

$$\begin{aligned}&\mathtt{G}\neg\mathtt{fgruen}\ \vee\\ &\neg\mathtt{F}\Big(\ \mathtt{gedrueckt} \wedge \mathtt{frot} \wedge \mathtt{X}\big(\neg\mathtt{gedrueckt}\ \mathtt{U}\ (\neg\mathtt{frot} \wedge \mathtt{X}(\neg\mathtt{gedrueckt}\ \mathtt{U}\ \mathtt{fgruen}))\big)\ \vee\\ &\quad \neg\mathtt{frot} \wedge \neg\mathtt{gedrueckt} \wedge \mathtt{X}(\neg\mathtt{gedrueckt}\ \mathtt{U}\ \mathtt{fgruen})\ \Big)\end{aligned}$$

Im folgenden werden wir zeigen, dass dies kein Zufall ist.

Definition 4.14
Sei $\varphi \in \mathrm{PLTL}$. Wir definieren $\overleftarrow{\varphi}$ – die *Umkehrung* von φ – induktiv durch

$$\begin{array}{rcl}\overleftarrow{q} & := & q\\ \overleftarrow{\varphi \vee \psi} & := & \overleftarrow{\varphi} \vee \overleftarrow{\psi}\\ \overleftarrow{\mathtt{X}\varphi} & := & \mathtt{Y}\overleftarrow{\varphi}\\ \overleftarrow{\varphi\mathtt{U}\psi} & := & \overleftarrow{\varphi}\,\mathtt{S}\,\overleftarrow{\psi}\\ \overleftarrow{\varphi\mathtt{S}\psi} & := & \overleftarrow{\varphi}\,\mathtt{U}\,\overleftarrow{\psi}\end{array} \qquad \begin{array}{rcl}\overleftarrow{\neg q} & := & \neg q\\ \overleftarrow{\varphi \wedge \psi} & := & \overleftarrow{\varphi} \wedge \overleftarrow{\psi}\\ \overleftarrow{\mathtt{Y}\varphi} & := & \mathtt{X}\overleftarrow{\varphi}\\ \overleftarrow{\varphi\mathtt{R}\psi} & := & \overleftarrow{\varphi}\,\mathtt{H}\,\overleftarrow{\psi}\\ \overleftarrow{\varphi\mathtt{H}\psi} & := & \overleftarrow{\varphi}\,\mathtt{R}\,\overleftarrow{\psi}\end{array}$$

Sei $\pi = \ldots s_{-2}s_{-1}s_0s_1s_2\ldots$ ein zweiseitig unendlicher Lauf. Die Umkehrung von π entsteht durch Spiegelung: $\overleftarrow{\pi} := \ldots s_2s_1s_0s_{-1}s_{-2}\ldots$.

Lemma 4.11
Für alle $\varphi \in \mathrm{PLTL}$, alle zweiseitig unendlichen Läufe π und alle $i \in \mathbb{Z}$ gilt: $\pi, i \models \varphi$ gdw. $\overleftarrow{\pi}, -i \models \overleftarrow{\varphi}$.

Beweis Wird standardmäßig durch Induktion über den Formelaufbau bewiesen. ∎

Eine direkte Konsequenz daraus und der Tatsache, dass die Menge aller zweiseitig unendlichen Läufe trivialerweise unter Umkehrung abgeschlossen ist, ist das folgende Korollar.

Korollar 4.18
Für alle $\varphi \in \mathrm{PLTL}$ gilt: $\models \varphi$ gdw. $\models \overleftarrow{\varphi}$.

Lemma 4.12
In PLTL gelten neben den üblichen booleschen Distributivgesetzen die folgenden Äquivalenzen.

- $\mathtt{X}(\varphi \vee \psi) \equiv \mathtt{X}\varphi \vee \mathtt{X}\psi, \quad \mathtt{Y}(\varphi \vee \psi) \equiv \mathtt{Y}\varphi \vee \mathtt{Y}\psi$
- $\mathtt{X}(\varphi \wedge \psi) \equiv \mathtt{X}\varphi \wedge \mathtt{X}\psi, \quad \mathtt{Y}(\varphi \wedge \psi) \equiv \mathtt{Y}\varphi \wedge \mathtt{Y}\psi$
- $\mathtt{X}(\varphi \mathtt{U} \psi) \equiv (\mathtt{X}\varphi)\mathtt{U}(\mathtt{X}\psi), \quad \mathtt{Y}(\varphi \mathtt{U} \psi) \equiv (\mathtt{Y}\varphi)\mathtt{U}(\mathtt{Y}\psi)$
- $\mathtt{X}(\varphi \mathtt{R} \psi) \equiv (\mathtt{X}\varphi)\mathtt{R}(\mathtt{X}\psi), \quad \mathtt{Y}(\varphi \mathtt{R} \psi) \equiv (\mathtt{Y}\varphi)\mathtt{R}(\mathtt{Y}\psi)$
- $\mathtt{X}(\varphi \mathtt{S} \psi) \equiv (\mathtt{X}\varphi)\mathtt{S}(\mathtt{X}\psi), \quad \mathtt{Y}(\varphi \mathtt{S} \psi) \equiv (\mathtt{Y}\varphi)\mathtt{S}(\mathtt{Y}\psi)$
- $\mathtt{X}(\varphi \mathtt{H} \psi) \equiv (\mathtt{X}\varphi)\mathtt{H}(\mathtt{X}\psi), \quad \mathtt{Y}(\varphi \mathtt{H} \psi) \equiv (\mathtt{Y}\varphi)\mathtt{H}(\mathtt{Y}\psi)$
- $\mathtt{XY}\varphi \equiv \varphi \equiv \mathtt{YX}\varphi$
- $\varphi \mathtt{U}(\psi_1 \vee \psi_2) \equiv \varphi \mathtt{U} \psi_1 \ \vee \ \varphi \mathtt{U} \psi_2, \quad \varphi \mathtt{S}(\psi_1 \vee \psi_2) \equiv \varphi \mathtt{S} \psi_1 \ \vee \ \varphi \mathtt{S} \psi_2$
- $(\varphi_1 \wedge \varphi_2)\mathtt{U}\psi \equiv \varphi_1 \mathtt{U} \psi \ \wedge \ \varphi_2 \mathtt{U} \psi, \quad (\varphi_1 \wedge \varphi_2)\mathtt{S}\psi \equiv \varphi_1 \mathtt{U} \psi \ \wedge \ \varphi_2 \mathtt{S} \psi$
- $(\varphi_1 \vee \varphi_2)\mathtt{R}\psi \equiv \varphi_1 \mathtt{R} \psi \ \vee \ \varphi_2 \mathtt{R} \psi, \quad (\varphi_1 \vee \varphi_2)\mathtt{H}\psi \equiv \varphi_1 \mathtt{H} \psi \ \vee \ \varphi_2 \mathtt{H} \psi$
- $\varphi \mathtt{R}(\psi_1 \wedge \psi_2) \equiv \varphi \mathtt{R} \psi_1 \ \wedge \ \varphi \mathtt{R} \psi_2, \quad \varphi \mathtt{H}(\psi_1 \wedge \psi_2) \equiv \varphi \mathtt{H} \psi_1 \ \wedge \ \varphi \mathtt{H} \psi_2$

Beweis Übung. ■

Definition 4.15
Eine PLTL-Formel φ heißt *rein*, wenn sie in positiver Normalform ist und für alle $\psi \in \mathit{Sub}(\varphi)$ gilt:

- Wenn $\psi = \mathtt{X}\psi'$, dann ist ψ' ein Literal oder eine X-Formel.
- Wenn $\psi = \mathtt{Y}\psi'$, dann ist ψ' ein Literal oder eine Y-Formel.
- Wenn $\psi = \psi_1 \mathtt{U} \psi_2$ oder $\psi = \psi_1 \mathtt{S} \psi_2$, dann ist ψ_1 eine Disjunktion und ψ_2 eine Konjunktion von Literalen, X-, Y-, U-, S-, R- oder H-Formeln.
- Wenn $\psi = \psi_1 \mathtt{R} \psi_2$ oder $\psi = \psi_1 \mathtt{H} \psi_2$, dann ist ψ_1 eine Konjunktion und ψ_2 eine Disjunktion von Literalen, X-, Y-, U-, S-, R- oder H-Formeln.

Lemma 4.13
Jeder PLTL-Formel φ ist äquivalent zu einer reinen PLTL-Formel φ'.

Beweis Laut Lemma 4.10 ist jedes φ äquivalent zu einem φ'' in positiver Normalform. Mithilfe der Äquivalenzen aus Lemma 4.12 lässt sich dann sukzessive φ'' in ein reines φ' umwandeln. ■

Lemma 4.14
Für alle $\varphi, \psi, \alpha, \beta \in \mathrm{PLTL}$ gilt:

$$\begin{aligned}\beta\ \mathtt{U}\big(\alpha \wedge (\varphi\ \mathtt{S}\ \psi)\big) \quad \equiv \quad & \alpha \wedge (\varphi\ \mathtt{S}\ \psi) && \vee\\ & \beta\ \mathtt{U}\ (\alpha \wedge \psi) && \vee\\ & (\varphi\ \mathtt{S}\ \psi) \wedge (\beta \wedge \varphi)\ \mathtt{U}\ (\alpha \wedge \varphi) && \vee\\ & \beta\ \mathtt{U}\Big(\beta \wedge \psi \wedge \mathtt{X}\big((\beta \wedge \varphi)\ \mathtt{U}\ (\alpha \wedge \varphi)\big)\Big)\end{aligned}$$

Beweis Übung. ■

Lemma 4.15
Für alle $\varphi, \psi, \alpha, \beta \in \mathrm{PLTL}$ gilt:

$$\begin{aligned}\beta\ \mathtt{U}\big(\alpha \wedge (\varphi\ \mathtt{H}\ \psi)\big) \quad \equiv \quad & \alpha \wedge (\varphi\ \mathtt{H}\ \psi) && \vee\\ & (\varphi\ \mathtt{H}\ \psi) \wedge (\beta \wedge \psi)\ \mathtt{U}\ (\alpha \wedge \psi) && \vee\\ & \beta\ \mathtt{U}\ (\alpha \wedge \varphi \wedge \psi) && \vee\\ & \beta\ \mathtt{U}\ \Big(\beta \wedge \varphi \wedge \psi \wedge \mathtt{X}\big((\beta \wedge \psi)\ \mathtt{U}\ (\alpha \wedge \psi)\big)\Big)\end{aligned}$$

Beweis Übung. ■

Lemma 4.16
Für alle $\varphi, \psi, \alpha, \beta \in \mathrm{PLTL}$ gilt:

$$\begin{aligned}\big(\beta \wedge (\varphi\ \mathtt{S}\ \psi)\big)\ \mathtt{R}\ \alpha \quad \equiv \quad & \mathtt{G}\alpha && \vee\\ & \varphi\ \mathtt{S}\ \psi\ \wedge\ (\alpha \wedge \varphi)\ \mathtt{U}\ (\alpha \wedge \beta \wedge \varphi) && \vee\\ & \alpha\ \mathtt{U}\ (\alpha \wedge \beta \wedge \psi) && \vee\\ & \alpha\ \mathtt{U}\ \Big(\alpha \wedge \psi \wedge \mathtt{X}\big((\alpha \wedge \varphi)\ \mathtt{U}\ (\alpha \wedge \beta \wedge \varphi)\big)\Big)\end{aligned}$$

Beweis Übung. ■

Lemma 4.17
Für alle $\varphi, \psi, \alpha, \beta \in \mathrm{PLTL}$ gilt:

$$\begin{aligned}\big(\beta \wedge (\varphi\ \mathtt{H}\ \psi)\big)\ \mathtt{R}\ \alpha \quad \equiv \quad & \mathtt{G}\alpha && \vee\\ & \varphi\ \mathtt{H}\ \psi\ \wedge\ (\alpha \wedge \psi)\ \mathtt{U}\ (\alpha \wedge \beta \wedge \psi) && \vee\\ & \alpha\ \mathtt{U}\ (\alpha \wedge \beta \wedge \varphi \wedge \psi) && \vee\\ & \alpha\ \mathtt{U}\ \Big(\alpha \wedge \varphi \wedge \psi \wedge \mathtt{X}\big((\alpha \wedge \psi)\mathtt{U}(\alpha \wedge \beta \wedge \psi)\big)\Big)\end{aligned}$$

Beweis Übung. ■

Definition 4.16
Eine PLTL-Formel heißt

- *Zukunftsformel*, wenn sie aus Literalen nur mit den Operatoren $\wedge$, $\vee$, `X`, `U` und `R`
- *Vergangenheitsformel*, wenn sie aus Literalen nur mit den Operatoren $\wedge$, $\vee$, `Y`, `S` und `H`

aufgebaut ist. Eine rein aussagenlogische Formel bezeichnen wir auch als *Gegenwartsformel*.

Eine Formel, die eine boolesche Kombination aus Vergangenheits-, Gegenwarts- und Zukunftsformeln ist, nennen wir *separiert*.

Satz 4.14
Jede PLTL-Formel φ ist äquivalent zu einem separierten φ'.

Beweis Sei $\varphi \in$ PLTL. Laut Lemma 4.13 existiert ein reines φ', so dass $\varphi \equiv \varphi'$. In φ' kommen die temporalen Operatoren `X` und `Y` nur vor atomaren Literalen vor. Falls φ' nicht separiert ist, dann muss es eine Unterformel haben, die von einem der folgenden 16 Schemata ist.

$(\mathtt{U_S})$	$\beta\ \mathtt{U}\ \big(\alpha \wedge (\varphi\ \mathtt{S}\ \psi)\big)$	$(\mathtt{S_U})$	$\beta\ \mathtt{S}\ \big(\alpha \wedge (\varphi\ \mathtt{U}\ \psi)\big)$
$(\mathtt{U_H})$	$\beta\ \mathtt{U}\ \big(\alpha \wedge (\varphi\ \mathtt{H}\ \psi)\big)$	$(\mathtt{S_R})$	$\beta\ \mathtt{S}\ \big(\alpha \wedge (\varphi\ \mathtt{R}\ \psi)\big)$
$(\mathtt{_SU})$	$\big(\beta \vee (\varphi\ \mathtt{S}\ \psi)\big)\ \mathtt{U}\ \alpha$	$(\mathtt{_US})$	$\big(\beta \vee (\varphi\ \mathtt{U}\ \psi)\big)\ \mathtt{S}\ \alpha$
$(\mathtt{_HU})$	$\big(\beta \vee (\varphi\ \mathtt{H}\ \psi)\big)\ \mathtt{U}\ \alpha$	$(\mathtt{_RS})$	$\big(\beta \vee (\varphi\ \mathtt{R}\ \psi)\big)\ \mathtt{S}\ \alpha$
$(\mathtt{R_S})$	$\beta\ \mathtt{R}\ \big(\alpha \vee (\varphi\ \mathtt{S}\ \psi)\big)$	$(\mathtt{H_U})$	$\beta\ \mathtt{H}\ \big(\alpha \vee (\varphi\ \mathtt{U}\ \psi)\big)$
$(\mathtt{R_H})$	$\beta\ \mathtt{R}\ \big(\alpha \vee (\varphi\ \mathtt{H}\ \psi)\big)$	$(\mathtt{H_R})$	$\beta\ \mathtt{H}\ \big(\alpha \vee (\varphi\ \mathtt{R}\ \psi)\big)$
$(\mathtt{_SR})$	$\big(\beta \wedge (\varphi\ \mathtt{S}\ \psi)\big)\ \mathtt{R}\ \alpha$	$(\mathtt{_UH})$	$\big(\beta \wedge (\varphi\ \mathtt{U}\ \psi)\big)\ \mathtt{H}\ \alpha$
$(\mathtt{_HR})$	$\big(\beta \wedge (\varphi\ \mathtt{H}\ \psi)\big)\ \mathtt{R}\ \alpha$	$(\mathtt{_RH})$	$\big(\beta \wedge (\varphi\ \mathtt{R}\ \psi)\big)\ \mathtt{H}\ \alpha$

Ist diese vom Schema $(\mathtt{U_S})$,$(\mathtt{U_H})$,$(\mathtt{_SR})$ oder $(\mathtt{_HR})$, dann lässt sie sich mithilfe der Lemmas 4.14–4.17 durch eine äquivalente Unterformel ersetzen, in der die Verschachtelung der Vergangenheits- und Zukunftsoperatoren aufgelöst wurde.

Beachte, dass die übrigen Fälle $(\mathtt{_SU})$, $(\mathtt{_HU})$, $(\mathtt{R_S})$ und $(\mathtt{R_H})$ der linken Spalte negationsdual zu den obigen Fällen sind, und somit ebenfalls mithilfe der Lemmas 4.14–4.17 behandelt werden können. Die Fälle der rechten Spalte lassen sich dann mithilfe von Korollar 4.18 auf den jeweiligen Fall der linken Spalte in derselben Zeile zurückführen.

Das Ergebnis dieser einmaligen Ersetzung ist eine PLTL-Formel φ', deren Verschachtelungstiefe zwischen Vergangenheits- und Zukunftsoperatoren geringer ist als die von φ, die aber u.U. nicht rein ist. Dieses Verfahren kann jedoch iterativ auf φ' angewandt werden, bis eine separierte Formel entstanden ist. ■

Korollar 4.19
Über einseitig unendlichen Läufen gilt PLTL $\equiv$ LTL, wenn Formeln nur im Anfang eines Laufes interpretiert werden.

Beweis Die Richtung LTL $\leq$ PLTL ist trivial. Zur Umkehrung lässt sich mithilfe von Satz 4.14 jede PLTL-Formel in eine boolesche Kombination aus Vergangenheits-, Gegenwarts- und Zukunftsformeln transferieren. Über einseitig unendlichen Läufen nur im Anfangszustand interpretiert ist der Vergangenheitsteil jedoch irrelevant und kann eliminiert werden. Das Resultat ist eine LTL-Formel. ■

Beachte, dass die LTL-Formeln, die von dem in Korollar 4.19 skizzierten Algorithmus produziert werden, i.A. wesentlich größer als die originalen PLTL-Formeln sind. Dies muss teilweise so sein, denn man kann zeigen, dass es PLTL-Formeln φ_n, $n \in \mathbb{N}$, gibt, zu denen die kleinsten äquivalenten LTL-Formeln eine Größe $2^{\Omega(|\varphi_n|)}$ haben [LMS02].

Zum Abschluss präsentieren wir ein Resultat über die Komplexität von PLTL.

Satz 4.15
Das Erfüllbarkeits-, Allgemeingültigkeits- und das Model Checking Problem für PLTL ist jeweils PSPACE-vollständig.

Beweis Übung. ■