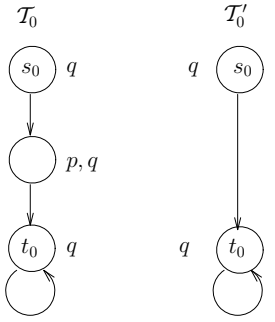
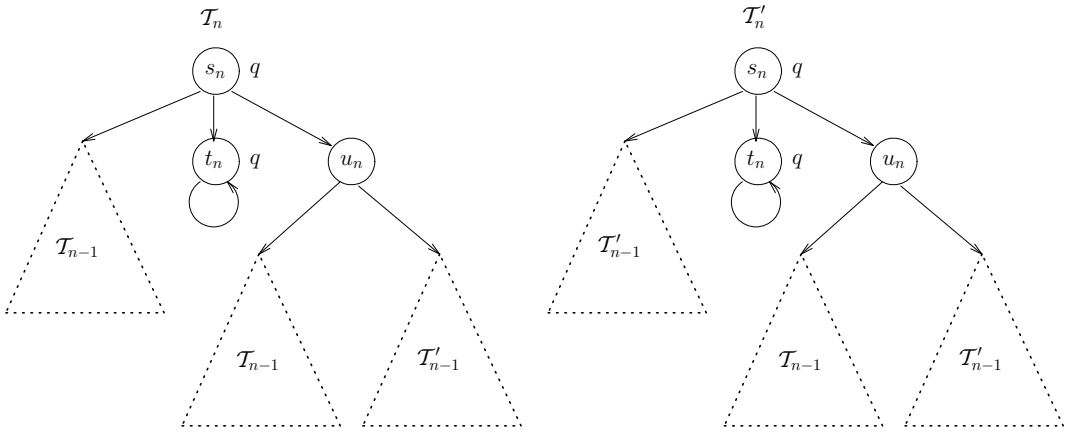
Beweis Wir zeigen, dass es keine UCTL-Formel gibt, die äquivalent zu der UCTL$^+$-Formel $\mathtt{E}(\mathtt{F}p \wedge \mathtt{G}q)$ ist. Dazu definieren wir wiederum induktiv zwei Familien von Transitionssystemen $\mathcal{T}_n, \mathcal{T}'_n$, $n \in \mathbb{N}$. Für $n = 0$ sehen diese folgendermaßen aus.



Und für $n > 0$ werden sie folgendermaßen konstruiert.



Erstens gilt offensichtlich $\mathcal{T}_n, s_n \models \mathtt{E}(\mathtt{F}p \wedge \mathtt{G}q)$ und $\mathcal{T}'_n, s_n \not\models \mathtt{E}(\mathtt{F}p \wedge \mathtt{G}q)$ für alle $n \in \mathbb{N}$. Ersteres gilt wegen dem Lauf, der rekursiv immer nach $\mathcal{T}_{n-1}$ absteigt und letztendlich $\mathcal{T}_0$ durchläuft. Zweiteres gilt, weil kein Lauf durch ein $\mathcal{T}'_n$, der genauso rekursiv absteigt, immer q erfüllt. Jeder Lauf, der sofort in ein t_n mündet, erfüllt niemals p, und jeder Lauf, der durch ein u_n führt, kann nicht überall q erfüllen.

Wir bemerken, dass außerdem gilt:

1. Alle Zustände t_i in beliebigen $\mathcal{T}_n$ oder $\mathcal{T}'_n$, $n \geq i$, sind bisimilar.
2. $\mathcal{T}_n, u_n \sim \mathcal{T}'_n, u_n$ für alle $n \geq 1$.
3. Jeder Lauf durch $\mathcal{T}_n$ oder $\mathcal{T}'_n$ durchläuft schließlich nur noch einen Zustand t_i für ein $i \leq n$.

Als nächstes zeigen wir durch Induktion über n, dass für alle $\varphi \in$ UCTL mit $td(\varphi) \geq n$ gilt: $\mathcal{T}_n, s_n \models \varphi$ gdw. $\mathcal{T}'_n, s_n \models \varphi$. O.B.d.A. können wir davon ausgehen, dass φ nur aus atomaren Propositionen mit Disjunktionen, Negationen und den temporalen Operatoren `EX`, `EG` und `EF` aufgebaut ist. Die Behauptung ist für atomare Propositionen sofort ersichtlich und folgt für die booleschen Operatoren sofort aus der Induktionshypothese. Es bleiben die drei Fälle der temporalen Operatoren übrig.

Fall $\varphi = \mathtt{EX}\psi$. Angenommen es gilt $\mathcal{T}_n, s_n \models \varphi$. Dann gibt es drei Unterfälle: (a) $\mathcal{T}_n, t_n \models \psi$, (b) $\mathcal{T}_n, u_n \models \psi$ oder (c) $\mathcal{T}_{n-1}, s_{n-1} \models \psi$. Liegt (a) oder (b) vor, dann lässt sich sofort mithilfe der Bemerkungen (1) oder (2) schließen, dass auch $\mathcal{T}'_n, t_n \models \psi$ bzw. $\mathcal{T}'_n, u_n \models \psi$ gilt. Liegt Fall (c) vor, dann beachte, dass $td(\psi) = td(\varphi) - 1$ gilt, weswegen sich die Induktionshypothese anwenden lässt und $\mathcal{T}'_{n-1}, s_{n-1} \models \psi$ liefert. Dann gilt aber sicherlich auch $\mathcal{T}'_n, s_n \models \varphi$. Die Rückrichtung läuft vollkommen analog ab.

Fall $\varphi = \mathtt{EG}\psi$. Angenommen es gilt $\mathcal{T}_n, s_n \models \varphi$. Aus der Bemerkung (3) von oben folgt dann insbesondere (a) $\mathcal{T}_n, s_n \models \psi$ und (b) $\mathcal{T}_i, t_i \models \psi$ oder $\mathcal{T}'_i, t_i \models \psi$ für ein $i \leq n$. Jetzt wenden wir die Beobachtung (1) von oben auf (b) an und erhalten auch $\mathcal{T}'_n, t_n \models \psi$. Auf (a) wenden wir die Induktionshypothese an, da $td(\psi) < td(\varphi)$ ist, und erhalten ebenfalls $\mathcal{T}'_n, s_n \models \psi$. Dann gilt aber auch $\mathcal{T}'_n, s_n \models \varphi$. Die Umkehrung wird ebenfalls vollkommen analog bewiesen.

Fall $\varphi = \mathtt{EF}\psi$. Angenommen es gilt $\mathcal{T}_n, s_n \models \varphi$. Dann gibt es also einen Zustand x in $\mathcal{T}_n$, so dass $\mathcal{T}_n, x \models \psi$ gilt, da jeder Zustand in $\mathcal{T}_n$ von s_n aus erreichbar ist. Wir müssen mehrere Fälle unterscheiden.

- Falls $x = s_n$ dann folgt $\mathcal{T}'_n, s_n \models \psi$ aus der Induktionshypothese für ψ.
- Falls $x = u_i$ für ein $i \leq n$, dann folgt $\mathcal{T}'_n, s_n \models \psi$ aus Bemerkung (2) von oben.
- Falls $x = t_i$ für ein $i \leq n$, dann folgt $\mathcal{T}'_n, t_n \models \psi$ aus Bemerkung (1) von oben.
- Falls x von u_n aus erreichbar ist, dann gilt auch $\mathcal{T}'_n, x \models \psi$, da x auch in derselben Form in $\mathcal{T}'_n$ vorhanden ist.
- Falls x von s_{n-1} aus erreichbar ist, dann gibt es ein y, welches von u_n aus erreichbar ist, so dass $x \sim y$. Da der von u_n aus erreichbare Teil ebenfalls in $\mathcal{T}'_n$ vorhanden ist, gilt somit auch hier $\mathcal{T}'_n, y \models \psi$.

In allen Fällen gibt es also einen Zustand y in $\mathcal{T}'_n$, der ψ erfüllt, womit auch $\mathcal{T}'_n, s_n \models \varphi$ gezeigt ist. Die Rückrichtung wird wiederum genauso bewiesen.

Der Rest des Beweises geht wie üblich vor. Angenommen, es gäbe eine UCTL Formel φ, so dass $\varphi \equiv \mathtt{E}(\mathtt{F}p \wedge \mathtt{G}q)$. Sei $n := td(\varphi)$. Dann müsste $\mathcal{T}_n, s_n \models \varphi$ und $\mathcal{T}'_n, s_n \not\models \varphi$ gelten, was aber der soeben bewiesenen Aussage widerspricht, dass diese beiden nicht von UCTL-Formeln der temporalen Tiefe $\leq n$ unterschieden werden können. ∎

5.5. Fair CTL

Da die Restriktion der Syntax von CTL* auf CTL$^+$ nicht den gewünschten Effekt – insbesondere höhere Ausdrucksstärke als CTL – hatte, erweitern wir jetzt gezielt die Syntax von CTL um wünschenswerte Eigenschaften.

Definition 5.6
Sei $\mathcal{P}$ eine Menge von Propositionen. Ein *Fairnessprädikat* über $\mathcal{P}$ ist eine positive boolesche Kombination Φ von Formeln der Form $\mathtt{GF}l$, wobei l ein Literal über $\mathcal{P}$ ist. Die Syntax von *Fair CTL* (FCTL) lässt in der Syntax von CTL auch um Fairnessprädikate relativierte Laufquantoren zu.

$$\varphi \;:=\; q \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mathtt{EX}\varphi \mid \mathtt{AX}\varphi \mid \mathtt{E}_\Phi(\varphi \mathtt{U} \psi) \mid \mathtt{A}_\Phi(\varphi \mathtt{U} \psi) \mid \mathtt{E}_\Phi(\varphi \mathtt{R} \psi) \mid \mathtt{A}_\Phi(\varphi \mathtt{U} \psi)$$

wobei $q \in \mathcal{P}$ und Φ ein Fairnessprädikat über $\mathcal{P}$ ist. Die temporale Tiefe $td(\varphi)$ einer FCTL-Formel definieren wir hier genauso wie bei CTL – Fairnessprädikate werden also nicht berücksichtigt.

Die Semantik ist eindeutig durch Einbettung in CTL* gegeben:

$$\begin{aligned} \mathtt{E}_\Phi(\psi) &:= \mathtt{E}(\Phi \wedge \psi) \\ \mathtt{A}_\Phi(\psi) &:= \mathtt{A}(\Phi \rightarrow \psi) \end{aligned}$$

Beispiel 5.5
Betrachte ein Szenario, in dem mehrere Prozesse $P_1, \ldots, P_n$ auf eine Ressource zugreifen. Diese darf aber nur von einem einzigen Prozess zur selben Zeit benutzt werden. Jeder Prozess P_i kann über die Proposition s_i signalisieren, dass er auf die Ressource zugreifen möchte. Mit den Propositionen e_i und f_i wird angedeutet, dass Prozess P_i den Zugriff erhält, bzw. die Ressource wieder freigibt. Eine korrekte Implementierung eines solchen Protokolls, welches auch *wechselseitiger Ausschluss* oder *mutual exclusion* genannt wird, sollte sicherlich die folgenden CTL-Formeln erfüllen.

$$\mathtt{AG}\Big(\bigwedge_{i=1}^{n} e_i \rightarrow \mathtt{A}\big(f_i \mathtt{R}(\bigwedge_{j=1}^{n} \neg e_j)\big)\Big)$$

Dies besagt, dass niemals ein Prozess die Ressource erhält, wenn ein anderer sie noch nicht freigegeben hat. Außerdem möchte man sagen, dass jeder Prozess, der die Ressource haben möchte, sie irgendwann auch einmal erhält.

$$\mathtt{AG}(\bigwedge_{i=1}^{n} s_i \rightarrow \mathtt{AF}e_i)$$

Diese Formel ist aber im Allgemeinen nicht erfüllt, denn es kann evtl. Läufe geben, bei denen ein Prozess die Ressource erhält, sie aber nicht mehr freigibt. Somit kann auf solchen Läufen kein anderer Prozess sie erhalten. Dennoch sollte deswegen die Implementierung des Protokolls, welches lediglich die Signale der Prozesse registriert und die Ressource, wenn möglich, zuteilt, nicht als inkorrekt angesehen werden. Vielmehr ist es der eine Prozess, der die Ressource nicht wieder freigibt, der inkorrekt ist.

FCTL bietet eine verfeinerte Möglichkeit, diese Art der Korrektheit zu spezifizieren. Wir wollen als Fairnessprädikat eine Formel benutzen, die "unendlich oft wird die Ressource einem Prozess zugeteilt" ausdrückt. Beachte, dass gilt:

$$\mathtt{GF}(\bigvee_{i=1}^{n} e_i) \quad \equiv \quad \bigvee_{i=1}^{n} \mathtt{GF}e_i$$

womit solch ein Fairnessprädikat Φ gefunden ist. Dann lässt sich obige CTL-Formel verfeinern zu

$$\mathtt{AG}(\bigwedge_{i=1}^{n} s_i \rightarrow \mathtt{A}_\Phi \mathtt{F} e_i)$$

5.5.1. Ausdrucksstärke

Satz 5.11
CTL $\lneq$ FCTL.

Beweis Die Inklusion gilt, da $\mathtt{tt}$ als Fairnessprädikat darstellbar ist, z.B. $\Phi := \mathtt{GF}q \vee \mathtt{GF}\neg q$. Dann ist $\mathtt{E}(\varphi \mathtt{U} \psi) \equiv \mathtt{E}_\Phi(\varphi \mathtt{U} \psi)$, etc.

Die Striktheit der Inklusion ist eine Konsequenz aus Satz 3.11. Angenommen, es würde CTL $\equiv$ FCTL gelten. Dann müsste es auch eine CTL-Formel geben, die äquivalent zu der FCTL-Formel $\mathtt{E}_{\mathtt{GF}q}(\mathtt{tt}\mathtt{U}\mathtt{tt})$ wäre. Diese ist aber äquivalent zu der CTL*-Formel $\mathtt{EGF}q$, deren Eigenschaft nicht in CTL ausgedrückt werden kann. ■

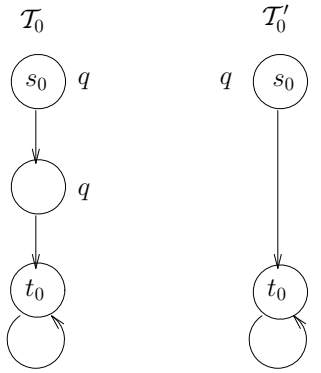
Beachte, dass ein Fairnessprädikat auch eine LTL-Formel ist, weswegen man sie direkt über Läufen interpretieren kann.

Lemma 5.5
Sei $\pi = s_0 s_1 \ldots$ ein Lauf. Für alle Fairnessprädikate Φ und alle $i \in \mathbb{N}$ gilt: $\pi \models \Phi$ gdw. $\pi^{(i)} \models \Phi$.

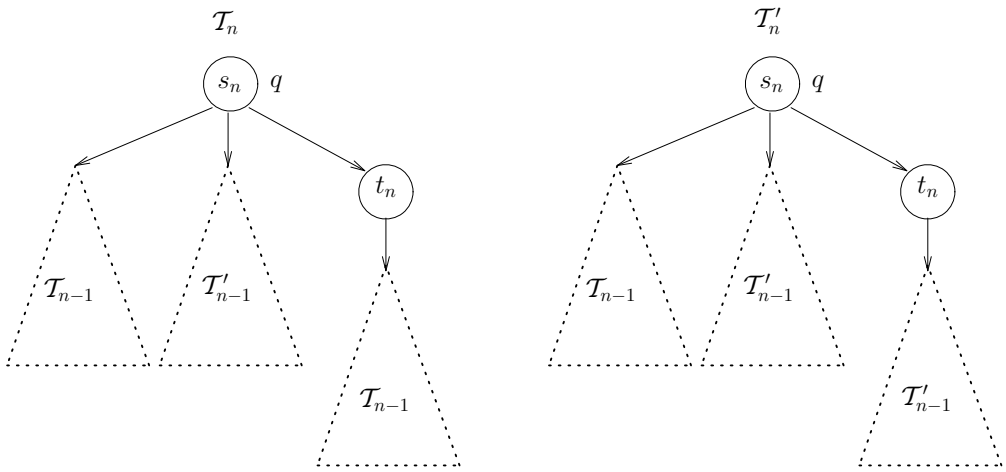
Beweis Dies folgt sofort aus der Tatsache, dass ein endliches Anfangsstück eines Laufs nichts daran ändert, ob auf dem Lauf unendlich oft eine Proposition (nicht) gilt. Es ist also leicht zu sehen, dass für alle Literale l und alle $i \in \mathbb{N}$ gilt: $\pi \models \mathtt{GF}l$ gdw. $\pi^{(i)} \models \mathtt{GF}l$. Für allgemeine Fairnessprädikate folgt die Aussage dann leicht per Induktion über ihren booleschen Aufbau. ■

Satz 5.12
FCTL $\lneq$ CTL*.

Beweis Wir zeigen in der üblichen Weise, dass es keine FCTL-Formel gibt, die äquivalent zu der CTL*-Formel $\mathtt{AF}(q \wedge \mathtt{X}q)$ ist. Dazu konstruieren wir wiederum zwei Familien von Transitionssystemen $\mathcal{T}_n$ und $\mathcal{T}'_n$ für alle $n \in \mathbb{N}$ wie folgt. Für $n = 0$ sehen diese folgendermaßen aus.



Für $n > 0$ sind diese induktiv definiert als



Man erkennt leicht, dass für alle $n \in \mathbb{N}$ gilt: $\mathcal{T}_n, s_n \models \mathtt{AF}(q \wedge \mathtt{X}q)$, aber $\mathcal{T}'_n, s_n \not\models \mathtt{AF}(q \wedge \mathtt{X}q)$.

Als nächstes zeigen wir durch Induktion über den Aufbau von FCTL-Formeln φ, dass für alle $n \in \mathbb{N}$ mit $td(\varphi) \leq n$ gilt: $\mathcal{T}_n, x \models \varphi$ gdw. $\mathcal{T}'_n, x \models \varphi$, wobei $x \in \{s_n, t_n\}$. Die Aussage des Satzes ergibt sich daraus dann wieder in der üblichen Weise.

Für atomare Propositionen ist dies wiederum sofort ersichtlich, und die Fälle der booleschen Operatoren werden sofort aus der Induktionshypothese hergeleitet. Es bleiben noch die Fälle $\mathtt{EX}\psi$, $\mathtt{E}_\Phi(\psi_1 \mathtt{U} \psi_2)$ und $\mathtt{E}_\Phi(\psi_1 \mathtt{R} \psi_2)$ für beliebige Fairnessprädikate Φ zu zeigen. Wir beschränken uns hier auf die Zustände s_n. Für die t_n wird dies alles analog bewiesen.

Fall $\varphi = \mathtt{EX}\psi$: Es gilt $\mathcal{T}_n, s_n \models \varphi$ gdw. $\mathcal{T}_n, t_n \models \psi$ oder $\mathcal{T}_{n-1}, s_{n-1} \models \psi$ oder $\mathcal{T}'_{n-1}, s_{n-1} \models \psi$. Auf den ersten Fall lässt sich die Induktionshypothese anwenden. Damit erhält man sofort $\mathcal{T}'_n, s_n \models \varphi$ und umgekehrt.

Für die verbleibenden Fälle bemerken wir folgendes. Sei Φ ein beliebiges Fairnessprädikat. Dann gilt für alle $n \in \mathbb{N}$ und für alle Läufe π, π' in $\mathcal{T}_n$ oder $\mathcal{T}'_n$: $\pi \models \Phi$ gdw. $\pi' \models \Phi$. Dies ist eine Konsequenz aus Lemma 5.5, da alle solche Läufe von der Form $\sigma(t_0)^\omega$ für ein beliebiges Präfix σ sind, und sich somit zwei verschiedene Läufe nur durch ein endliches Anfangsstück unterscheiden.

Sei Φ also ein beliebiges Fairnessprädikat. Dann sind entweder alle Läufe in diesen Transitionssystemen oder keiner Modell von Φ. D.h. über diesen Familien von Transitionssystemen ist FCTL nur so ausdrucksstark wie CTL und es reicht aus, die übrigen Fälle durch die einfachen CTL-Konstrukte $\mathtt{E}(\psi_1 \mathtt{U} \psi_2)$ bzw. $\mathtt{E}(\psi_1 \mathtt{R} \psi_2)$ zu ersetzen.

Fall $\varphi = \mathtt{E}(\psi_1 \mathtt{U} \psi_2)$: Angenommen $\mathcal{T}_n, s_n \models \mathtt{E}(\psi_1 \mathtt{U} \psi_2)$. Dann gilt $\mathcal{T}_n, s_n \models \psi_2$ oder es gibt einen Lauf π, der $\psi_1 \mathtt{U} \psi_2$ erfüllt. Im ersten Fall erhatlen wir $\mathcal{T}'_n, s_n \models \varphi$ direkt aus der Induktionshypothese. Ansonsten müssen wir drei Fälle unterscheiden. Falls π sofort in $\mathcal{T}_{n-1}$ oder $\mathcal{T}'_{n-1}$ mündet, dann finden wir denselben Lauf auch in $\mathcal{T}'_n$ und können daraus ebenfalls $\mathcal{T}'_n, s_n \models \varphi$ schließen. Falls π über t_n in $\mathcal{T}_{n-1}$ mündet, dann gibt es wiederum

zwei Unterfälle: Wenn $t_n \models \psi_2$, dann gilt mit der Induktionshypothese für t_n und ψ_2 sowie für s_n und ψ_1 auch $\mathcal{T}'_n \models \varphi$. Wenn ψ_2 erst in $\mathcal{T}_{n-1}$ erfüllt wird, dann findet sich aber auch ein Pfad, der sofort – und nicht über t_n – in $\mathcal{T}_{n-1}$ mündet und $\psi_1 \mathtt{U} \psi_2$ erfüllt. Dieser existiert aber auch in $\mathcal{T}'_n$, womit die Behauptung auch in diesem Unterfall bewiesen ist. Die Rückrichtung wird analog gezeigt.

Fall $\varphi = \mathtt{E}(\psi_1 \mathtt{R} \psi_2)$: Dies geht genauso durch multiple Fallunterscheidungen wie im vorherigen Fall. ■

5.5.2. Komplexität

Es zeigt sich, dass FCTL eine bessere Einschränkung von CTL* bzgl. Komplexität und Ausdrucksstärke als CTL$^+$ ist. Aus den Sätzen 5.5 und 5.11 folgt natürlich CTL$^+ \leq$ FCTL. Andererseits kann man zeigen, dass die Model Checking Komplexität von FCTL gleich der von CTL$^+$, nämlich Δ_2-vollständig ist. Insbesondere gilt das folgende Resultat.

Satz 5.13
Model Checking FCTL ist NP-hart und co-NP-hart.

Dass dies nicht an den Fairnessoperatoren $\mathtt{GF}l$ alleine liegt, zeigt folgendes Resultat.

Satz 5.14
Das Model Checking Problem für FCTL mit Fairnessprädikaten der Form $\bigwedge_i \bigvee_j \mathtt{GF} l_{ij}$ ist P-vollständig.

Dass man durch diese eingeschränkte Form keine Ausdrucksstärke verliert, sollte klar sein: Jedes Fairnessprädikat lässt sich äquivalent in diese Form übersetzen. Dabei kann allerdings die resultierende Formel exponentiell größer werden.

6. Der modale μ-Kalkül

Zur Erinnerung: Wir haben zuerst HML betrachtet und gesehen, dass dies als temporale Logik bei weitem zu ausdrucksschwach ist. HML-Formeln können Transitionssysteme ab einer bestimmten Tiefe nicht mehr unterscheiden. Um dieses Defekt zu beheben haben wir die temporale Logik CTL betrachtet, die Operatoren zur Verfügung stellt, mit denen man "beliebig tief" in ein Transitionssystem schauen kann. Dasselbe gilt für LTL. Es hat sich dann gezeigt, dass sich die Semantik dieser Operatoren als Fixpunkt einer bestimmten Gleichung – der sogenannten Abwicklung – über Mengen von Zuständen darstellen lässt. Zum Abschluss betrachten wir noch eine Logik, die diese Idee in expliziter Form benutzt. Der modale μ-Kalkül erweitert HML um Operatoren, deren Semantik der kleinste bzw. größte Fixpunkt einer durch die Formel explizit gegebenen Abwicklung ist.

6.1. Syntax und Semantik

Definition 6.1
Sei $\mathcal{V} = \{X, Y, \ldots\}$ eine höchstens abzählbar unendliche Menge von Variablen, $\mathcal{P}$ wie üblich eine Menge von Propositionen und Σ eine endliche Menge von Aktionennamen. Formeln des modalen μ-Kalküls $\mathcal{L}_\mu$ sind gegeben durch die folgende Grammatik.

$$\varphi \quad ::= \quad q \mid X \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \neg\varphi \mid \langle a \rangle \varphi \mid [a]\varphi \mid \mu X.\varphi \mid \nu X.\varphi$$

wobei $q \in \mathcal{P}$, $a \in \Sigma$ und $X \in \mathcal{V}$. Im folgenden schreiben wir auch σ als Platzhalter für die Quantoren μ oder ν.

Wir benutzen wieder die üblichen Abkürzungen $\mathtt{tt} := q \vee \neg q$ für ein $q \in \mathcal{P}$, $\mathtt{ff} := \neg\mathtt{tt}$, $\varphi \rightarrow \psi := \neg\varphi \vee \psi$, etc.

Die Menge $Sub(\varphi)$ der Unterformeln von φ ist definiert wie üblich, z.B. $Sub(\mu X.\psi) = \{\mu X.\psi\} \cup Sub(\psi)$ etc. Die Begriffe *freie Variable* und *geschlossene Formel* etc. sind wie üblich definiert. Dabei binden die Quantoren μ und ν eine Variable. So ist z.B. Z in der Formel

$$\mu X.\langle a \rangle \neg \nu Y.\neg((Z \wedge \neg X) \vee \neg\langle a \rangle Y) \tag{6.1}$$

frei, X und Y sind gebunden. Sei $free(\varphi)$ die Menge aller freien Variablen von φ.

Eine Formel φ heißt *wohlbenannt*, wenn für alle $\sigma X.\psi$ und $\sigma Y.\psi'$ gilt: Wenn $X = Y$ dann $\psi = \psi'$. In anderen Worten: Jede Variable wird höchstens einmal quantifiziert. Ist dies der Fall, dann existiert eine Funktion $fp_\varphi : \mathcal{V} \cap Sub(\varphi) \rightarrow Sub(\varphi)$, die einer gebundenen Variable X, die in φ vorkommt, ihre Fixpunktdefinition $\sigma X.\psi$ zuordnet. Der *Fixpunkttyp* einer Variablen X ist der Quantor in $fp_\varphi(X)$, also μ oder ν.

Eine Formel φ heißt *wohlgeformt*, wenn jede gebundene Variable X unter einer geraden Anzahl von Negationen in $fp_\varphi(X)$ vorkommt. So ist z.B. die obige Formel (6.1) nicht wohlgeformt.

Im folgenden gehen wir davon aus, dass jede $\mathcal{L}_\mu$-Formel wohlbenannt und wohlgeformt ist. Ersteres ist keine Einschränkung, da offensichtlich jede Formel durch eindeutiges Umbenennen von gebundenen Variablen in eine äquivalente und wohlbenannte Formel transformiert werden kann – auch wenn deren Semantik noch nicht definiert wurde. Zweiteres ist gewissermaßen auch keine Einschränkung, da man einer nicht wohlgeformten Formel keine Semantik in vernünftiger Weise geben kann.

Der modale μ-Kalkül wird wie HML über allgemeinen, evtl. auch kantenbeschrifteten und nicht notwendigerweise totalen Transitionssystemen interpretiert.

Definition 6.2
Sei $\mathcal{T} = (\mathcal{S}, \{\xrightarrow{a} \mid a \in \Sigma\}, \lambda)$ ein Transitionssystem. Eine *Umgebung* ist eine Abbildung $\rho : \mathcal{V} \to 2^{\mathcal{S}}$, mit deren Hilfe freie Variablen in einer Formel durch eine Menge von Zuständen in $\mathcal{S}$ interpretiert werden. Wir schreiben $\rho[X \mapsto T]$ für die Umgebung, die definiert ist durch

$$\rho[X \mapsto T](Y) \;=\; \begin{cases} T & , \text{ falls } Y = X \\ \rho(Y) & , \text{ sonst} \end{cases}$$

Die Semantik einer $\mathcal{L}_\mu$-Formel – in Bezug auf $\mathcal{T}$ und eine Umgebung ρ – ist dann induktiv definiert wie folgt.

$$\begin{aligned}
[\![q]\!]^{\mathcal{T}}_\rho &:= \{s \in \mathcal{S} \mid q \in \lambda(s)\} \\
[\![X]\!]^{\mathcal{T}}_\rho &:= \rho(X) \\
[\![\varphi \vee \psi]\!]^{\mathcal{T}}_\rho &:= [\![\varphi]\!]^{\mathcal{T}}_\rho \cup [\![\psi]\!]^{\mathcal{T}}_\rho \\
[\![\varphi \wedge \psi]\!]^{\mathcal{T}}_\rho &:= [\![\varphi]\!]^{\mathcal{T}}_\rho \cap [\![\psi]\!]^{\mathcal{T}}_\rho \\
[\![\neg\varphi]\!]^{\mathcal{T}}_\rho &:= \mathcal{S} \setminus [\![\varphi]\!]^{\mathcal{T}}_\rho \\
[\![\langle a\rangle\varphi]\!]^{\mathcal{T}}_\rho &:= \{s \in \mathcal{S} \mid \exists t \in \mathcal{S} : s \xrightarrow{a} t \text{ und } t \in [\![\varphi]\!]^{\mathcal{T}}_\rho\} \\
[\![[a]\varphi]\!]^{\mathcal{T}}_\rho &:= \{s \in \mathcal{S} \mid \forall t \in \mathcal{S} : \text{ wenn } s \xrightarrow{a} t \text{ dann } t \in [\![\varphi]\!]^{\mathcal{T}}_\rho\} \\
[\![\mu X.\varphi]\!]^{\mathcal{T}}_\rho &:= \bigcap\{T \subseteq \mathcal{S} \mid [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto T]} \subseteq T\} \\
[\![\nu X.\varphi]\!]^{\mathcal{T}}_\rho &:= \bigcup\{T \subseteq \mathcal{S} \mid T \subseteq [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto T]}\}
\end{aligned}$$

Wir schreiben auch $\mathcal{T}, s \models_\rho \varphi$, falls $s \in [\![\varphi]\!]^{\mathcal{T}}_\rho$. Beachte, dass die Semantik einer geschlossenen Formel φ nicht von der Umgebung ρ abhängt. In solch einem Fall schreiben wir dann auch einfach $\mathcal{T}, s \models \varphi$, bzw. $[\![\varphi]\!]^{\mathcal{T}}$.

Zwei nicht notwendigerweise geschlossene $\mathcal{L}_\mu$-Formeln φ und ψ sind äquivalent, $\varphi \equiv \psi$, falls für alle Transitionssysteme $\mathcal{T}$ und alle Umgebungen ρ gilt: $[\![\varphi]\!]^{\mathcal{T}}_\rho = [\![\psi]\!]^{\mathcal{T}}_\rho$. Ein φ ist *allgemeingültig*, geschrieben $\models \varphi$, falls gilt: $\varphi \equiv \mathtt{tt}$.

Eine $\mathcal{L}_\mu$-Formel φ ist in *positiver Normalform*, wenn das Negationssymbol in ihr nur vor atomaren Propositionen vorkommt. Um wie üblich zu zeigen, dass positive Normalform keine Einschränkung an die Ausdrucksstärke der Logik stellt, brauchen wir eine weitere Notation. Mit $\varphi[\psi/\chi]$ bezeichnen wir die Formel, die aus φ entsteht, wenn in ihr jedes Vorkommen von χ durch ψ ersetzt wird.

Lemma 6.1
Jede wohlgeformte und geschlossene $\mathcal{L}_\mu$-Formel φ ist äquivalent zu einem φ' in positiver Normalform.

Beweis Negationssymbole, die nicht vor Propositionen auftreten, können mithilfe der folgenden Äquivalenzen nach innen geschoben werden.

$$\begin{array}{rcl@{\qquad}rcl} \neg(\varphi \vee \psi) & \equiv & \neg\varphi \wedge \neg\psi & \neg\langle a\rangle\varphi & \equiv & [a]\neg\varphi \\ \neg(\varphi \wedge \psi) & \equiv & \neg\varphi \vee \neg\psi & \neg[a]\varphi & \equiv & \langle a\rangle\neg\varphi \\ \neg\mu X.\varphi & \equiv & \nu X.\neg\varphi[\neg X/X] & \neg\nu X.\varphi & \equiv & \mu X.\neg\varphi[\neg X/X] \\ \neg\neg\varphi & \equiv & \varphi \end{array}$$

Alle Äquivalenzen außer den Dualitäten der Fixpunktoperatoren sind leicht einzusehen. Wir zeigen explizit für eine der Fixpunktäquivalenzen, dass diese gilt. Die andere folgt dann aus der letzten Äquivalenz und dieser. Sei $\mathcal{T}$ ein Transitionssystem mit Zustandsmenge $\mathcal{S}$, ρ eine Umgebung.

$$\begin{aligned} [\![\neg\mu X.\varphi]\!]^{\mathcal{T}}_\rho &= \mathcal{S} \setminus \bigcap\{T \mid [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto T]} \subseteq T\} \\ &= \bigcup\{\mathcal{S} \setminus T \mid [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto T]} \subseteq T\} \\ &= \bigcup\{\mathcal{S} \setminus T \mid \mathcal{S} \setminus [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto T]} \supseteq \mathcal{S} \setminus T\} \\ &= \bigcup\{\mathcal{S} \setminus T \mid \mathcal{S} \setminus T \subseteq \mathcal{S} \setminus [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto T]}\} \\ &= \bigcup\{\mathcal{S} \setminus T \mid \mathcal{S} \setminus T \subseteq \mathcal{S} \setminus [\![\varphi[\neg X/X]]\!]^{\mathcal{T}}_{\rho[X\mapsto \mathcal{S}\setminus T]}\} \\ &= \bigcup\{\mathcal{S} \setminus T \mid \mathcal{S} \setminus T \subseteq [\![\neg\varphi[\neg X/X]]\!]^{\mathcal{T}}_{\rho[X\mapsto \mathcal{S}\setminus T]}\} \\ &= \bigcup\{T' \mid T' \subseteq [\![\neg\varphi[\neg X/X]]\!]^{\mathcal{T}}_{\rho[X\mapsto T']}\} \\ &= [\![\nu X.\neg\varphi[\neg X/X]]\!]^{\mathcal{T}}_\rho \end{aligned}$$

Beachte, dass $\{\mathcal{S}\setminus T \mid T \subseteq \mathcal{S}\} = 2^{\mathcal{S}}$ ist. Es bleibt lediglich zu erkennen, dass sich die Negationssymbole vor Variablen jeweils restlos aufheben, da aufgrund der Wohlgeformtheit und der Geschlossenheit zwischen jeder Variable und ihrem dazugehörigen Fixpunktquantor eine gerade Anzahl von Negationssymbolen vorkommt. Außerdem erzeugt dass Hineinschieben eines weiter außen vorkommenden Negationssymbols mit den Äquivalenzen für Fixpunkte innerhalb einer Formel $\sigma X.\psi$ immer zwei neue Negationssymbole, womit weiterhin dort nur eine gerade Anzahl vor jeder Variable steht. ∎

Lemma 6.2
Für alle $\varphi \in \mathcal{L}_\mu$ in positiver Normalform, alle $X \in \mathcal{V}$, alle Transitionssysteme $\mathcal{T}$ mit Zustandsmenge $\mathcal{S}$ ist die Abbildung $T \mapsto [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto T]}$ vom Typ $2^{\mathcal{S}} \to 2^{\mathcal{S}}$ monoton in Bezug auf die Ordnung $\subseteq$.

Beweis Übung. ∎

Der folgende, für die Fixpunkttheorie fundamentale Satz, benutzt dieses Lemma. Er ist trotz seiner Wichtigkeit nicht allzu schwer zu beweisen. Wir präsentieren ihn jedoch hier lediglich, um die Definition der $\mathcal{L}_\mu$-Semantik nachträglich zu motivieren, und verzichten auf den Beweis.

Satz 6.1 (Knaster/Tarski [Tar55])
Sei $\mathcal{T}$ ein Transitionssystem, ρ eine Umgebung und $\varphi \in \mathcal{L}_\mu$. Dann ist $[\![\mu X.\varphi]\!]^{\mathcal{T}}_\rho$ der kleinste (bzgl. $\subseteq$) Fixpunkt der Abbildung $T \mapsto [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto T]}$. Genauso ist $[\![\nu X.\varphi]\!]^{\mathcal{T}}_\rho$ der größte Fixpunkt dieser Abbildung.

Dieser Satz hat unmittelbare Konsequenzen. Z.B. dass man die propositionalen Konstanten $\mathtt{tt}$ und $\mathtt{ff}$ auch über einem $\mathcal{P} = \emptyset$ definieren kann: $\mathtt{tt} \equiv \nu X.X$, $\mathtt{ff} \equiv \mu X.X$.

Korollar 6.1
Für alle $\varphi \in \mathcal{L}_\mu$, alle $X \in \mathcal{V}$ und alle σ gilt $\sigma X.\varphi \equiv \varphi[\sigma X.\varphi/X]$.

Korollar 6.2
Für alle $\varphi \in \mathcal{L}_\mu$ und alle $X \in \mathcal{V}$ gilt: $\models \mu X.\varphi \to \nu X.\varphi$.

Beweis Sei $\mathcal{T}$ ein Transitionssystem. Wegen Kor. 6.1 gilt für alle ρ

$$[\![\mu X.\varphi]\!]^{\mathcal{T}}_\rho \;=\; [\![\varphi[\mu X.\varphi/X]]\!]^{\mathcal{T}}_\rho$$

Die linke Seite der Gleichung hängt nicht von $\rho(X)$ ab, also auch die rechte Seite nicht. Somit gilt auch

$$[\![\mu X.\varphi]\!]^{\mathcal{T}}_\rho \;\subseteq\; [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto [\![\mu X.\varphi]\!]^{\mathcal{T}}_\rho]} \tag{6.2}$$

Dann folgt aber $[\![\mu X.\varphi]\!]^{\mathcal{T}}_\rho \subseteq [\![\nu X.\varphi]\!]^{\mathcal{T}}_\rho$, da wegen (6.2) gilt

$$[\![\mu X.\varphi]\!]^{\mathcal{T}}_\rho \;\in\; \{T \subseteq \mathcal{S} \mid T \subseteq [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto T]}\}$$

also auch

$$[\![\mu X.\varphi]\!]^{\mathcal{T}}_\rho \;\subseteq\; \bigcup\{T \subseteq \mathcal{S} \mid T \subseteq [\![\varphi]\!]^{\mathcal{T}}_{\rho[X\mapsto T]}\} \;=\; [\![\nu X.\varphi]\!]^{\mathcal{T}}_\rho$$

was zu zeigen war. ∎

Im folgenden definieren wir strukturelle Maße einer Formel, die bei der Komplexität des Model Checkings eine große Rolle spielen.

Definition 6.3
Die *Fixpunkttiefe* einer Formel φ, $fpd(\varphi)$, ist – ähnlich der temporalen Tiefe bei Logiken der vorigen Kapitel – die maximale Anzahl von Fixpunktquantoren auf einem Pfad des Syntaxbaums von φ.

Dass die Fixpunkttiefe kein gutes Maß für die Komplexität einer Formel ist, zeigen die folgenden Beispiele.