

Beweis Gäbe es eine solche, dann wäre $2\text{-EXPTIME} = \text{EXPTIME}$ wegen Satz 5.3. Dies ist aber nicht der Fall. ■

6.4. Ausdrucksstärke

Wie oben erwähnt, kann man Lemma 6.3 auch auf unendliche Transitionssysteme erweitern. Dazu müssen Approximanden für trans-finite Ordinalzahlen definiert werden. Dann erhält man volle Fixpunktelimination: Jede $\mathcal{L}_\mu$ -Formel ist äquivalent zu einer (in-finitären) Formel ohne Fixpunktoperatoren, also eine ∞ -HML-Formel.

Satz 6.6

$\mathcal{L}_\mu \preceq \infty\text{-HML}$.

Dass diese Inklusion strikt ist, folgt aus einem anderen fundamentalen Resultat, welches wir nur erwähnen: Der modale μ -Kalkül ist genauso ausdrucksstark wie das bisimulations-invariante Fragment von Monadischer Logik 2. Stufe bzw. endliche Rabin-Automaten auf unendlichen Bäumen [EJ91, Eme85, JW96, Rab69]. Damit erhält man, dass jede von einer $\mathcal{L}_\mu$ -Formel ausgedrückte Eigenschaft nur *regulär* im formalsprachlichen Sinne ist. Es gibt jedoch auch Eigenschaften, die nicht von endlichen Baumautomaten ausgedrückt werden können, z.B. die sogenannte *uniform inevitability*: *Es gibt ein $k \in \mathbb{N}$, so dass auf allen Läufen nach k Schritten q gilt.* Man kann zeigen, dass diese Eigenschaft nicht durch solche Automaten und somit auch nicht durch eine $\mathcal{L}_\mu$ -Formel beschrieben werden kann [Eme87]. In ∞ -HML ist dies jedoch einfach:

$$\bigvee_{k \in \mathbb{N}} \underbrace{[-] \dots [-]}_{k \text{ mal}} q$$

Korollar 6.8

Für alle Transitionssysteme $\mathcal{T}$, Zustände s, t und alle geschlossenen $\varphi \in \mathcal{L}_\mu$ gilt: wenn $s \sim t$, dann $\mathcal{T}, s \models \varphi$ gdw. $\mathcal{T}, t \models \varphi$.

Als nächstes präsentieren wir die Antwort auf eine Frage, die ca. 15 Jahre lang offen war. *Kann man mit mehr Alternierung mehr ausdrücken?* Dies ist wichtig, da die Alternierungstiefe das bestimmende Maß in der Komplexität des Model Checking Problems für $\mathcal{L}_\mu$ ist.

Satz 6.7

Für alle $k \in \mathbb{N}$ gilt: $\mathcal{L}_\mu^k \preceq \mathcal{L}_\mu^{k+1}$.

Dies wurde zuerst von Bradfield [Bra96] und Lenzi [Len96] unabhängig voneinander gezeigt. Bradfield hat später noch eine vereinfachtere Version seines Beweises nachgelegt [Bra98]. Der einfachste Beweis dieses Resultats stammt allerdings von Arnold [Arn99], der die Korrespondenz zwischen $\mathcal{L}_\mu$ -Formel und alternierenden Baumautomaten mit Paritätsbedingungen, bzw. die Model Checking Spiele für $\mathcal{L}_\mu$ [Sti95] und in eleganter

6. Der modale μ -Kalkül

Weise Banach's Fixpunktsatz benutzt, um zu zeigen, dass die sogenannten Walukiewicz-Formeln

$$\varphi_n := \mu X_1. \nu X_2. \mu X_3. \dots \sigma X_n. \bigwedge_{i=1}^n ((p \wedge q_i \rightarrow \langle - \rangle X_i) \wedge (\neg p \wedge q_i \rightarrow [-] X_i))$$

der Alternierungstiefe n jeweils nicht äquivalent zu einer Formel der Alternierungstiefe $n - 1$ sind.

Dieses Resultat gilt über allgemeinen Transitionssystemen bzw. aus Gründen der Bismulationsinvarianz über Bäumen. Es stellt sich die Frage, ob es eingeschränkte Klassen von Strukturen gibt, so dass $\mathcal{L}_\mu$ auf diesen Strukturen keine echte Alternierungshierarchie besitzt. Das Einschränken der Anzahl der Nachfolger eines Zustandes ist hinunter bis zu 2 möglich, ohne dass die Hierarchie kollabiert: Arnolds Beweis zeigt, dass sie über unendlichen, binären und nur knotenbeschrifteten Bäumen immer noch existiert. Darunter ist dies aber nicht mehr der Fall.

Satz 6.8

Für alle $\varphi \in \mathcal{L}_\mu$ existiert ein alternierungsfreies $\varphi' \in \mathcal{L}_\mu^1$, so dass auf linearen Strukturen gilt: $\varphi \equiv \varphi'$.

Die besten oberen Schranken an die Größe eines solchen φ' sind jedoch exponentiell in $ad(\varphi)$.

Definition 6.6

Eine $\mathcal{L}_\mu$ -Formel φ heißt *bewacht*, wenn für alle gebundenen Variablen $X \in Sub(\varphi)$ gilt: X tritt in $fp_\varphi(X)$ nur unterhalb eines $\langle a \rangle$ oder $[a]$ auf.

Lemma 6.5

Für jedes $\varphi \in \mathcal{L}_\mu$ existiert ein bewachtes φ' , so dass $\varphi \equiv \varphi'$.

Beweis Per Induktion über den Formelaufbau. Alle Fälle außer den der Fixpunktooperatoren sind entweder trivial oder folgen sofort aus der Induktionshypothese.

Sei $\varphi = \mu X. \psi(X)$. Wegen der Induktionshypothese können wir ψ bereits als bewacht annehmen. Falls X in φ ebenfalls bewacht ist, dann ist φ insgesamt bewacht. Sei also angenommen, dass X in φ unbewacht vorkommt. Dann gibt es zwei Fälle zu unterscheiden.

Im ersten Fall kommt X in ψ nur unter booleschen Operatoren vor. Im zweiten Fall gibt es eine Unterformel $\sigma Y. \gamma(Y, X)$, so dass X unbewacht in dieser vorkommt. Wir behandeln zuerst den zweiten Fall und führen diesen auf den ersten zurück.

Nach Induktionsvoraussetzung kommt Y in $\sigma Y. \gamma(Y, X)$ nur bewacht vor. Dann benutzen wir die Äquivalenz $\sigma Y. \gamma(Y, X) \equiv \gamma(\sigma Y. \gamma(Y, X), X)$ und erhalten eine Formel, in der X nur unbewacht außerhalb des Fixpunktoperators vorkommt.

Dies führt uns zurück zu dem ersten Fall. Es liegt also o.B.d.A. eine Formel $\mu X. \psi(X)$ vor, in der alle unbewachten Vorkommen von X nur unter booleschen Operatoren in ψ

sind. Mithilfe der Distributivgesetze für boolesche Operatoren gibt es $\beta, \alpha_1, \dots, \alpha_n$ für ein $n \in \mathbb{N}$, so dass

$$\mu X.\psi(X) \equiv \mu X.\beta(X) \wedge \bigwedge_{i=1}^n (X \vee \alpha_i(X)) \equiv \mu X.\beta(X) \wedge (X \vee \bigwedge_{i=1}^n \alpha_i(X))$$

wobei alle Vorkommen von X in $\beta(X)$ und $\alpha_1(X), \dots, \alpha_n(X)$ bewacht sind. Beachte, dass $\beta(X) = \mathbf{tt}$ und $\alpha_i(X) = \mathbf{ff}$ für jedes i möglich ist.

Wir behaupten nun, dass φ äquivalent ist zu der bewachten Formel $\mu X.\beta(X) \wedge \alpha(X)$, wobei $\alpha(X) := \bigwedge_{i=1}^n \alpha_i(X)$. D.h. wir müssen zeigen, dass gilt

$$\models \mu X.\beta(X) \wedge (X \vee \alpha(X)) \leftrightarrow \mu X.\beta(X) \wedge \alpha(X)$$

Wir zeigen zuerst einmal die Implikation von rechts nach links. Dazu reicht es wegen Satz 6.1 aus, Fixpunktinduktion anzuwenden und zu zeigen, dass gilt:

$$\models (\beta(X) \wedge \alpha(X))[\mu X.\beta(X) \wedge (X \vee \alpha(X)) / X] \rightarrow \mu X.\beta(X) \wedge (X \vee \alpha(X))$$

Dies ist aber aufgrund der Implikation $\models \beta(X) \wedge \alpha(X) \rightarrow \beta(X) \wedge (X \vee \alpha(X))$ und Korollar 6.1 sofort ersichtlich.

Es bleibt also noch zu zeigen, dass auch die Implikation von links nach rechts gilt. Wiederum kann man dazu Fixpunktinduktion verwenden und zeigt stattdessen, dass gilt:

$$\models (\beta(X) \wedge (X \vee \alpha(X)))[\mu X.\beta(X) \wedge \alpha(X) / X] \rightarrow \mu X.\beta(X) \wedge \alpha(X)$$

Sei $\varphi_0 := \mu X.\beta(X) \wedge \alpha(X)$. Wegen Korollar 6.1 gilt offensichtlich $\models \varphi_0 \leftrightarrow \beta(\varphi_0) \wedge \alpha(\varphi_0)$, also auch

$$\models \beta(\varphi_0) \wedge (\varphi_0 \vee \alpha(\varphi_0)) \rightarrow \beta(\varphi_0) \wedge ((\beta(\varphi_0) \wedge \alpha(\varphi_0)) \vee \alpha(\varphi_0))$$

Letzteres ist aber äquivalent zu $\beta(\varphi_0) \wedge \alpha(\varphi_0)$ und somit zu φ_0 . Damit ist auch die zweite Implikation bewiesen, und insgesamt ist gezeigt, dass φ äquivalent zu der bewachten Formel $\mu X.\beta(X) \wedge \alpha(X)$ ist.

Der Fall $\varphi = \nu X.\psi(X)$ wird analog gezeigt. ■

Definition 6.7

Ein Transitionssystem $\mathcal{T} = (\mathcal{S}, \{\xrightarrow{a} \mid a \in \Sigma\}, \lambda)$ heißt *terminierend*, wenn es nicht unendlich viele $s_i \in \mathcal{S}$ gibt, so dass für alle $i \in \mathbb{N}$ gilt: $s_i \xrightarrow{a} s_{i+1}$ für ein $a \in \Sigma$.

Lemma 6.6

Sei $\varphi \in \mathcal{L}_\mu$, $X \in \mathcal{V}$, $\mathcal{T} = (\mathcal{S}, \{\xrightarrow{a} \mid a \in \Sigma\}, \lambda)$ terminierend und $s \in \mathcal{S}$. Dann gilt für alle Umgebungen ρ : $\llbracket \mu X.\varphi \rrbracket_\rho^{\mathcal{T}} = \llbracket \nu X.\varphi \rrbracket_\rho^{\mathcal{T}}$.

Beweis Sei $\mathcal{T}$ terminierend, ρ eine Umgebung, $X \in \mathcal{V}$ und $\varphi \in \mathcal{L}_\mu$. Falls $X \notin \text{free}(\varphi)$ dann gilt die Behauptung trivialerweise. Ansonsten ist X in $\sigma X.\varphi$ gebunden, und wegen

6. Der modale μ -Kalkül

Lemma 6.5 können wir o.B.d.A. annehmen, dass X in φ nur unterhalb eines modalen Operators vorkommt.

Jetzt sei angenommen, dass $\llbracket \mu X.\varphi \rrbracket_\rho^T \neq \llbracket \nu X.\varphi \rrbracket_\rho^T$ gilt. Wegen Korollar 6.2 existiert also ein $s_0 \in \mathcal{S}$, so dass $s_0 \not\models_\rho \mu X.\varphi$ aber $s_0 \models_\rho \nu X.\varphi$. Zuerst wenden wir Korollar 6.1 an und erhalten

$$s_0 \not\models_\rho \varphi[\mu X.\varphi/X] \quad \text{und} \quad s_0 \models_\rho \varphi[\nu X.\varphi/X]$$

Wir zeigen jetzt durch Fallunterscheidung über den Aufbau von φ , dass dies nicht sein kann. Dies ist offensichtlich für den Fall $\varphi = Y$ mit $Y \neq X$.

Fall $\varphi = \psi_1 \vee \psi_2$. Also gibt es ein $i \in \{1, 2\}$, so dass $s_0 \models_\rho \psi_i[\nu X.\varphi/X]$, aber $s_0 \not\models_\rho \psi_i[\mu X.\varphi/X]$. Somit ist dieser Fall auf den einer kleineren Formel reduziert. Der Fall $\varphi = \psi_1 \wedge \psi_2$ ist analog.

Fall $\varphi = \sigma Y.\psi$. Hier wenden wir wieder Korollar 6.1 an und erhalten $s_0 \not\models_\rho \psi[\sigma Y.\psi/Y][\mu X.\varphi/X]$ und $s_0 \models_\rho \psi[\sigma Y.\psi/Y][\nu X.\varphi/X]$. Diese Formeln sind zwar nicht syntaktisch kleiner, aber ψ liegt tiefer im Syntaxbaum als φ , womit das Problem wiederum verschoben wird.

Fall $\varphi = \langle a \rangle \psi$. Dann existiert ein $s_1 \in \mathcal{S}$, so dass $s_0 \xrightarrow{a} s_1$ und $s_1 \not\models_\rho \psi[\mu X.\varphi/X]$ und $s_1 \models_\rho \psi[\nu X.\varphi/X]$. Der Fall $\varphi = [a]\psi$ ist analog.

Es bleibt noch der Fall $\varphi = X$ übrig. Wegen obiger Annahme wurde in dieser Konstruktion mindestens ein modaler Operator durchlaufen, d.h. es gibt bereits $s_0, \dots, s_n$ für ein $n \geq 1$, so dass für alle $i = 0, \dots, n-1$: $s_i \xrightarrow{a} s_{i+1}$ für ein $a \in \Sigma$ und $s_n \not\models_\rho X[\mu X.\varphi/X]$ aber $s_n \models_\rho X[\nu X.\varphi/X]$. Also $s_n \not\models_\rho \mu X.\varphi$ aber $s_n \models_\rho \nu X.\varphi$.

Dieses Argument kann man jetzt iterieren. Entweder es wird irgendwann eine atomare Proposition q und ein $s \in \mathcal{S}$ erreicht, so dass $s \not\models_\rho q[\mu X.\varphi/X]$ und $s \models_\rho q[\nu X.\varphi/X]$ gilt. Dies ist der einzige Fall, der oben nicht behandelt wurde. Er ist aber auch offensichtlich ein Widerspruch.

Also lässt sich dieses Argument unendlich lange iterieren. Dann hat man aber unendlich viele $s_i \in \mathcal{S}$ gefunden, so dass $s_i \xrightarrow{a} s_{i+1}$ für alle $i \in \mathbb{N}$ und ein $a \in \Sigma$ gilt. Dies ist aber ein Widerspruch zu der Annahme, dass $\mathcal{T}$ terminierend ist. Wir schließen daraus, dass doch $\llbracket \mu X.\varphi \rrbracket_\rho^T = \llbracket \nu X.\varphi \rrbracket_\rho^T$ gelten muss. ■

Korollar 6.9

Für alle $\varphi \in \mathcal{L}_\mu$ existiert ein alternierungs-freies $\varphi' \in \mathcal{L}_\mu^1$, so dass auf terminierenden Strukturen gilt: $\varphi \equiv \varphi'$.

Beweis Ersetze in φ z.B. jedes ν durch μ . Die resultierende Formel φ' ist dadurch sicherlich alternierungsfrei, und wegen Lemma 6.6 auf terminierenden Transitionssystemen auch äquivalent zu φ . ■

6.5. CTL* als Fragment des modalen μ -Kalküls

Ziel dieses Abschnitts ist es zu zeigen, dass sich jede CTL*-definierbare Eigenschaft auch in $\mathcal{L}_\mu$ ausdrücken lässt. Dazu müssen wir eine äquivalenzerhaltende Übersetzung angeben. Beachte, dass diese insbesondere erfüllbarkeitserhaltend ist, und dann wegen

Korollar 6.7 nicht polynomiell sein kann. In der Tat verlangt diese Übersetzung ein wenig technisches Werkzeug.

Im folgenden bezeichnen wir einen Lauf eines Transitionssystems als Pfad. Zur Erinnerung: Ein nicht-deterministischer endlicher Automat (NFA) ist ein Tupel $\mathcal{A} = (Q, \Sigma, q_0, \delta, F)$, das benutzt wird, um Sprachen von endlichen Wörtern zu erkennen. Ein endlicher Pfad $s_0, \dots, s_n$ in einem knotenbeschrifteten Transitionssystem $\mathcal{T} = (\mathcal{S}, \rightarrow, \lambda)$ mit $\lambda : \mathcal{S} \rightarrow 2^{\mathcal{P}}$ induziert in natürlicher Weise ein endliches Wort über $\Sigma := 2^{\mathcal{P}}$. Eine Menge von endlichen Pfaden Π heißt *regulär*, wenn es einen NFA $\mathcal{A}$ gibt, der genau die von Pfaden in Π induzierten Wörter akzeptiert.

Um Automaten sinnvoll für CTL*-definierbare Eigenschaften verwenden zu können, müssen sie auf unendlichen Pfade operieren.

Definition 6.8

Sei $\mathcal{P}$ eine endliche Menge von Propositionen. Ein *nichtdeterministischer Büchi-Automat* (NBA) ist ein Tupel $\mathcal{A} = (Q, 2^{\mathcal{P}}, q_0, \delta, F)$, wobei

- Q eine endliche Menge von Zuständen ist,
- $2^{\mathcal{P}}$ das Alphabet des Automaten ist,
- $q_0 \in Q$ der Anfangszustand des Automaten ist,
- $\delta : Q \times 2^{\mathcal{P}} \rightarrow 2^Q$ die Übergangsrelation darstellt,
- $F \subseteq Q$ die Menge der Endzustände ist.

Normalerweise lässt man ein beliebiges, endliches Alphabet Σ zu. Da wir NBAs aber nur auf $\mathcal{P}$ -beschrifteten Pfaden eines Transitionssystems operieren lassen, benutzen wir hier gleich die spezialisierte Version mit $\Sigma = 2^{\mathcal{P}}$. NBAs sehen also syntaktisch genauso aus wie endliche Automaten, arbeiten aber auf unendlichen Objekten.

Definition 6.9

Sei $\pi = s_0, s_1, \dots$ ein Pfad mit Beschriftungsfunktion λ über $\mathcal{P}$. Ein *Lauf* eines NBA $\mathcal{A} = (Q, 2^{\mathcal{P}}, q_0, \delta, F)$ ist eine Folge $r = q_0, q_1, \dots$, so dass q_0 der Anfangszustand von $\mathcal{A}$ ist und für alle $i \in \mathbb{N}$ gilt: $q_{i+1} \in \delta(q_i, \lambda(s_i))$.

Ein Lauf $r = q_0, q_1, \dots$ heißt *akzeptierend*, wenn er unendlich oft einen Endzustand durchläuft, d.h. $\{q \mid q = q_i \text{ für unendliche viele } i\} \cap F \neq \emptyset$.

Sei $L(\mathcal{A}) = \{\pi \mid \text{es gibt einen akzeptierenden Lauf von } \mathcal{A} \text{ auf } \pi\}$. Eine Menge Π von Läufen heißt *Büchi-definierbar*, wenn es einen NBA $\mathcal{A}$ gibt, so dass $\Pi = L(\mathcal{A})$ ist.

Wir brauchen zwei fundamentale Sätze über Büchi-Automaten, die wir hier aber nicht beweisen wollen. Der erste stellt NBAs in Beziehung zu LTL-Formeln.

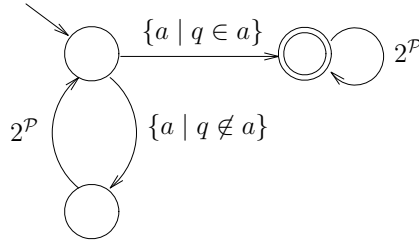
Satz 6.9

Für jede LTL-Formel φ existiert ein NBA $\mathcal{A}_\varphi$, so dass $L(\mathcal{A}_\varphi) = \llbracket \varphi \rrbracket$ und $|\mathcal{A}_\varphi| = 2^{O(|\varphi|)}$ gilt.

6. Der modale μ -Kalkül

Beispiel 6.6

Die Umkehrung gilt im übrigen nicht. So erkennt der folgende NBA z.B. die Menge aller Pfade, auf denen q an einer gerade Stelle gilt.



Der zweite Satz ist der sogenannte Satz von Büchi. Er stellt eine Beziehung zwischen den Büchi-definierbaren und den regulären Sprachen dar. Sei Π eine Menge endlicher Läufe. Mit Π^ω bezeichnen wir die unendliche Konkatenation von beliebigen Pfaden aus Π .

Satz 6.10

Sei Π eine Büchi-erkennbare Menge von unendlichen Pfaden über $\mathcal{P}$. Dann existiert ein $n \in \mathbb{N}$ und Mengen $U_1, V_1, \dots, U_n, V_n$ von endlichen Pfaden über $\mathcal{P}$, so dass $\Pi = \bigcup_{i=1}^n U_i V_i^\omega$ gilt.

Definition 6.10

Die Menge der *regulären Ausdrücke* über $2^{\mathcal{P}}$ ist die gegeben durch die Grammatik

$$\alpha ::= \epsilon \mid a \mid \alpha \cup \alpha \mid \alpha \alpha \mid \alpha^*$$

wobei $a \in 2^{\mathcal{P}}$. Die vom regulären Ausdruck α definierte Sprache $L(\alpha)$ – in der üblichen Weise definiert – können wir wieder wie bei NFAs als Menge von endlichen Pfaden auffassen.

Ein ω -regulärer Ausdruck α ist von der Form $\bigcup_{i=1}^n \alpha_i \beta_i^\omega$, wobei $n \in \mathbb{N}$ und die α_i und β_i jeweils reguläre Ausdrücke sind. Die von α definierte Sprache ist die Menge der unendlichen Pfade, die durch Vereinigung, Konkatenation und unendliche Iteration aus den jeweiligen $L(\alpha_i)$ und $L(\beta_i)$ entsteht.

Lemma 6.7

Für jede Büchi-definierbare Menge Π von unendlichen Läufen existiert ein ω -regulärer Ausdruck α , so dass $\Pi = L(\alpha)$ ist.

Beweis Sei Π Büchi-definierbar. Dann existiert also ein NBA $\mathcal{A}$ mit $L(\mathcal{A}) = \Pi$. Laut Satz 6.10 existieren reguläre Mengen von endlichen Pfaden $U_1, V_1, \dots, U_m, V_m$, so dass $\Pi = \bigcup_{i=1}^m U_i V_i^\omega$ ist. Da die regulären Ausdrücke genau die regulären Sprachen definieren, existieren reguläre Ausdrücke α_i, β_i für $i = 1, \dots, m$, so dass für den ω -regulären Ausdruck $\alpha := \bigcup_{i=1}^m \alpha_i \beta_i^\omega$ gilt: $L(\alpha) = \Pi$. ■

Darüberhinaus machen wir eine Bemerkung zu der Größe von α : Angenommen, Π wird von einem NBA mit n Zuständen definiert. Dann existieren für die U_i und V_i NFAs mit

jeweils höchstens n Zuständen. Damit ist die Größe der regulären Ausdrücke α_i und β_i jeweils beschränkt durch $O(n^3)$. Außerdem kann man $m \leq n$ annehmen. Insgesamt gilt also $|\alpha| = O(n^4)$.

Die vorherigen Resultate lassen sich nun zusammenfassen zu folgendem Korollar.

Korollar 6.10

Sei φ eine LTL-Formel über $\mathcal{P}$. Dann existiert ein ω -regulärer Ausdruck α_φ , so dass $L(\alpha_\varphi) = \llbracket \varphi \rrbracket$ und $|\alpha_\varphi| = 2^{O(|\varphi|)}$ gilt.

Als nächstes übersetzen wir ω -reguläre Ausdrücke in $\mathcal{L}_\mu$.

Lemma 6.8

Für jeden ω -regulären Ausdruck α existiert ein $\varphi_\alpha \in \mathcal{L}_\mu^2$, so dass für alle Transitionssysteme $\mathcal{T}$ mit Zustand s gilt: $\mathcal{T}, s \models \varphi_\alpha$ gdw. es gibt einen Pfad $\pi = s \dots$ so dass $\pi \in L(\alpha)$.

Beweis Sei $\alpha = \bigcup_{i=1}^n \alpha_i \beta_i^\omega$. Da $\mathcal{L}_\mu$ -Formeln unter Disjunktionen abgeschlossen sind und der existentielle Pfadquantor mit den Disjunktionen kommutiert, können wir o.B.d.A. $n = 1$ annehmen. Somit müssen wir nur noch φ_α für ein α von der Form $\alpha' \beta^\omega$ konstruieren, wobei α' und β reguläre Ausdrücke sind.

Wir geben eine Funktion tr an, die als Parameter eine Variable X und einen regulären Ausdruck γ erhält und folgende Spezifikation für alle Zustände s eines Transitionssystems erfüllt.

$$s \models_\rho tr_X(\gamma) \quad \text{gdw.} \quad \begin{array}{l} \text{es gibt einen Pfad } \pi = s \dots, \text{ so dass } \pi = \pi' \pi'' \text{ für ein } \pi' \in L(\gamma) \\ \text{und entweder } \pi' \text{ ist unendlich oder } \pi'' = t \dots \text{ mit } t \models_\rho X \end{array}$$

Beachte, dass γ in diesem Fall sowohl ein regulärer (π' nur endlich lang) als auch ω -regulärer Ausdruck (π' unendlich lang) sein kann. Intuitiv ist X ein Platzhalter für das, was gelten muss, wenn ein Wort in $L(\gamma)$ abgearbeitet ist.

$$\begin{aligned} tr_X(\epsilon) &:= X \\ tr_X(a) &:= \bigwedge_{q \in a} q \wedge \bigwedge_{q \notin a} \neg q \wedge \langle - \rangle X \quad \text{falls } a \in 2^{\mathcal{P}} \\ tr_X(\gamma_1 \vee \gamma_2) &:= tr_X(\gamma_1) \vee tr_X(\gamma_2) \\ tr_X(\gamma_1 \gamma_2) &:= tr_Y(\gamma_1)[tr_X(\gamma_2)/Y] \\ tr_X(\gamma^*) &:= \mu Y. X \vee tr_Y(\gamma) \\ tr_X(\gamma^\omega) &:= \nu Y. tr_Y(\gamma) \end{aligned}$$

wobei Y in jedem Fall eine bisher nicht benutzte Variable ist.

Die Korrektheit dieser Konstruktion zeigt man leicht durch Induktion über den Aufbau von γ . Beachte, dass außerdem gilt: $tr_X(\alpha' \beta^\omega)$ ist geschlossen und in $\mathcal{L}_\mu^2$. Letzteres liegt daran, dass ein ν -Operator nur durch den einzigen ω -Operator erzeugt wird. Innerhalb dessen kann es wegen evtl. Kleene-Sternen in β auch μ -Formeln geben, in denen die ν -Variable frei vorkommt. Da $tr_X(\beta^\omega)$ aber bereits geschlossen ist, können Kleene-Sterne in α' nicht zu weiterer Alternierung beitragen. ■

6. Der modale μ -Kalkül

Satz 6.11

$$\text{CTL}^* \preceq \mathcal{L}_\mu.$$

Beweis Wir benutzen wieder denselben Trick wie in Satz 5.2 beim Model Checking für CTL^* , welches wir durch Zerlegung der Formel auf das Model Checking Problem für LTL zurückgeführt haben.

Sei $\varphi_0 \in \text{CTL}^*$. O.B.d.A. können wir davon ausgehen, dass in φ_0 der universelle Pfadquantor **A** nicht vorkommt, sondern durch den existentiellen **E** und Negationen ersetzt wurde. Seien $\text{E}\psi_1, \dots, \text{E}\psi_m$ wiederum alle Unterformeln von φ_0 dieser Form in aufsteigender Reihenfolge bzgl. ihrer Größe. Da φ_0 eine Zustandsformel ist, gilt $\varphi_0 \equiv \text{E}\varphi_0$, und deswegen können wir davon ausgehen, dass $\varphi_0 = \psi_m$ ist.

Wir konstruieren nun schrittweise für $i = 1, \dots, m$ $\mathcal{L}_\mu$ -Formeln $\varphi_1, \dots, \varphi_m$, so dass für alle $i = 1, \dots, m$ gilt: $\varphi_i \equiv \text{E}\psi_i$. Beachte, dass für alle $i, j = 1, \dots, m$ gilt: Wenn $\text{E}\psi_j \in \text{Sub}(\psi_i)$, dann ist $j < i$. Also können wir immer davon ausgehen, dass ψ_i eine LTL-Formel ist. Darin auftretende pfadquantifizierte Zustandsformeln $\text{E}\psi_j$ können zuerst einmal durch neue, atomare Propositionen q_j ersetzt werden. Korollar 6.10 und Lemma 6.8 liefern dann die gewünschte $\mathcal{L}_\mu$ -Formel φ_i . Beachte, dass diese geschlossen ist. In ihr können die neuen Propositionen q_j wieder durch die bereits erzeugten und geschlossenen Formeln φ_j ersetzt werden.

Diese Konstruktion liefert letztendlich eine $\mathcal{L}_\mu$ -Formel φ' , so dass $\varphi_0 \equiv \varphi'$ gilt. Außerdem gilt $\varphi' \in \mathcal{L}_\mu^2$, denn jeder Schritt dieser Konstruktion liefert eine geschlossene Formel in $\mathcal{L}_\mu^2$. Dadurch ist auch die Zusammensetzung und deren Bereinigung in positiver Normalform in $\mathcal{L}_\mu^2$. Dies zeigt die Inklusion von CTL^* in $\mathcal{L}_\mu$. Die Striktheit dieser Inklusion ist eine direkte Konsequenz aus Satz 6.7, welcher u.a. $\mathcal{L}_\mu^2 \preceq \mathcal{L}_\mu$ zeigt. ■

Satz 6.11 liefert auch einen alternativen Beweis dafür, dass das Erfüllbarkeitsproblem für CTL^* in 2-EXPTIME ist. Aus den obigen Bemerkungen folgt, dass sich jede CTL^* -Formel φ äquivalent in eine $\mathcal{L}_\mu^2$ -Formel der Größe $2^{O(|\varphi|)}$ übersetzen lässt. Mit Satz 6.5 folgt dann, dass sich die Erfüllbarkeit von φ in Zeit $2^{2^{O(|\varphi|)}}$ überprüfen lässt.

Korollar 6.11

$$\text{CTL}^* \preceq \mathcal{L}_\mu^2.$$

Beweis Die Striktheit dieser stärkeren Inklusion ist eine Konsequenz aus obigem Bsp. 6.6. Damit und mit der Konstruktion aus dem Beweis von Satz 6.11 existiert eine $\mathcal{L}_\mu^2$ -Formel, welche besagt, dass es einen Pfad gibt, auf dem q an gerade Stelle gilt. Man kann sich leicht überlegen, dass dies nicht in CTL^* ausdrückbar ist. ■

Korollar 6.12

CTL^* und $\mathcal{L}_\mu^1$ sind unvergleichbar bzgl. der Ausdrucksstärke.

Beweis Die in Korollar 6.11 genannte Eigenschaft ist sogar in $\mathcal{L}_\mu^1$ ausdrückbar: $\mu X.q \vee \langle - \rangle \langle - \rangle X$. Zur anderen Richtung sei nur bemerkt, dass man zeigen kann, dass sich Fairnessprädikate bzw. Formeln der Form $\text{EGF}q$ nicht in $\mathcal{L}_\mu^1$ ausdrücken lassen. ■

7. Zusammenfassung

7.1. Komplexitäten

Die folgende Tabelle beschreibt noch einmal die Komplexitätsresultate für die in den vorigen Kapiteln vorgestellten Logiken. Einzelne Einträge beschreiben immer ein Vollständigkeitsresultat, wo also untere und obere Schranke zusammenfallen. Die Einträge mit einem Bereich beschreiben nur untere und obere Schranken, bei denen die genaue Komplexität noch unbekannt ist.

Wir beschränken uns auf das Model Checking Problem und das Erfüllbarkeitsproblem. Bei den Linearzeitlogiken ist ersteres als die Frage, ob alle Läufe eines Transitionssystems die gegebene Eigenschaft erfüllen, aufzufassen.

Die Komplexität des Allgemeingültigkeitsproblem ist in allen Fällen lediglich vollständig für das Komplement der Klasse, für die das Erfüllbarkeitsproblem vollständig ist. D.h. in fast allen Fällen ist dies dasselbe wie das Erfüllbarkeitsproblem.

Logik	Model Checking	Erfüllbarkeit
HML	P	PSPACE
CTL	P	EXPTIME
UCTL	P	EXPTIME
UCTL ⁻	P	EXPTIME
CTL ⁺	Δ_2	2-EXPTIME
UCTL ⁺	P ... Δ_2	EXPTIME ... 2-EXPTIME
FCTL	Δ_2	EXPTIME ... 2-EXPTIME
LTL	PSPACE	PSPACE
ULTL	PSPACE	PSPACE
SILTL	PSPACE	PSPACE
PLTL	PSPACE	PSPACE
MLTL	co-NP	NP
CTL*	PSPACE	2-EXPTIME
$\mathcal{L}_\mu^0, k \in \mathbb{N}$	P	PSPACE
$\mathcal{L}_\mu^k, k \geq 1$	P	EXPTIME
$\mathcal{L}_\mu$	P ... $\text{NP} \cap \text{co-NP}$	EXPTIME

7.2. Ausdrucksstärke

Die folgende Grafik stellt die in den vorigen Kapitel vorgestellten temporalen Logiken in Beziehung zueinander bzgl. ihrer Ausdrucksstärke. Alle eingezeichneten Linien ent-

7. Zusammenfassung

sprechen strikten Inklusionen. Logiken, die nicht transitiv miteinander verbunden sind, haben unvergleichbare Ausdrucksstärke.

