Fixpunktquantoren

Hauptseminar Fixpunkte
Ludwig-Maximilians-Universität München, WiSe 2004/05

Veranstalter: Dr. M. Lange, Dr. R. Matthes

Referent: Matthias Kling

1. Februar 2005

Inhaltsverzeichnis

1 Modelle

Die Strukturen, über die in den hier vorgestellten Logiken Aussagen getroffen werden (Modelle) sind gerichtete Graphen mit Markierungen an den Knoten und/oder den Kanten. Ein Überbegriff für solche Strukturen ist „Markiertes Zustandsübergangssystem“ (Labelled Transition System, LTS), da die Ecken als Zustände eines Systems und die Kanten als Übergänge von einem Zustand in einen anderen interpretiert werden können. Im folgenden werden „Knoten“, „Ecke“ und „Zustand“ vollkommen synonym gebraucht; ebenso „Kante“, „Übergang“ und „Transition“.
Je nach Logik werden wir eine etwas andere Variante verwenden. In diesem Abschnitt sollen die Begriffe etabliert werden, um diese Varianten unterscheiden und ohne viel Aufwand darauf Bezug nehmen zu können.
Häufig werden in LTSen ein oder mehrere Zustände als Anfangszustände ausgezeichnet, indem diese Menge der Anfangszustände in (den Formalismus für) die Struktur mit aufgenommen wird. Darauf verzichten wir hier, da uns besondere Anfangszustände nur am Rande beschäftigen werden.

1.1 Knotenbeschriftete Graphen

Eine knotenbeschriftetes LTS M ist ein Tripel (S, δ, l), wobei

- S eine Menge von Zuständen
- $\delta \subseteq S \times S$ eine Übergangs- oder Erreichbarkeitsrelation ist, die einem Zustand einen oder mehrere Nachfolgezustände zuordnet - oder auch nicht, dh. es kann auch Zustände ohne Nachfolger geben.
- $l : S \to 2^P$ eine Labelling-Funktion ist, die jedem Zustand eine Menge von (in diesem Zustand wahren) atomaren Formeln (Propositionen) zuordnet.

1.2 Kantenbeschriftete Graphen

Ein kantenbeschriftetes LTS M ist ein Tripel $(S, \mathcal{A}, \Delta)$, wobei

- S eine Menge von Zuständen
- $\mathcal{A}$ eine Menge von Markierungen für die Kanten; im Zusammenhang mit Prozessen auch Aktionen genannt. $\mathcal{A}$ selbst wird als das Alphabet von M bezeichnet.
- $\Delta = \{\, \delta_\alpha \subseteq S \times S \mid \alpha \in \mathcal{A} \}$ eine Familie von Übergangsrelationen δ_α, für jedes $\alpha \in \mathcal{A}$ eine (möglicher- und sinnvollerweise andere).

Es wäre auch möglich nur eine einzige Übergangsrelation $\delta' \subseteq S \times \mathcal{A} \times S$ zu verwenden. Für unsere Zwecke ist es aber praktischer so wie oben definiert.

1.3 Beschriftungen an Knoten und Kanten

Will man sowohl an Knoten als auch Kanten Markierungen haben, so lassen sich die beiden obigen Konzepte einfach kombinieren:
Ein kanten- und knotenbeschriftetes LTS ist ein Quadrupel $(S, \mathcal{A}, \Delta, l)$ mit $S, \mathcal{A}, \Delta$ und l

wie oben. Die Übergangsrelation δ aus dem Fall mit ausschließlich Knotenbeschriftungen erscheint dann als die Vereinungsmenge aller δ_α, dh.

$$\delta \;=\; \bigcup_{\alpha\in\mathcal{A}} \delta_\alpha \;=\; \{\, (s,t) \in S \times S \;\mid\; \text{es ex. } \alpha \in \mathcal{A}, \text{ sd. } (s,t) \in \delta_\alpha \,\}$$

Solche Strukturen werden wir als Modelle für den modalen μ-Kalkül verwenden, wobei wir δ nicht benötigen werden (weil in der Logik selbst entsprechendes ausgedrückt werden kann) und auf die Labellingfunktion l nur indirekt Bezug nehmen werden durch sog. Belegungen, die mit Hilfe von l konstruiert werden.

1.4 Berechnungsbäume und Pfade

Ein Pfad $\sigma = \sigma_0\sigma_1\sigma_2\ldots$ in M ist eine (potentiell) unendliche Sequenz von Zuständen $\sigma_i \in S$, sd. für alle $i \in \mathbf{N}$ gilt: $(\sigma_i, \sigma_{i+1}) \in \delta$. Da Pfade i.W. nur im Zusammenhang mit CTL von Bedeutung sind, wird auf eine Verfeinerung für kantenbeschriftete LTSe verzichtet

Wählt man einen Zustand aus und „wickelt" von diesem ausgehend die Struktur „ab", erhält man den zugehörigen *Berechnungsbaum* (computation tree), einen Baum mit möglicherweise unendlich langen Ästen aber, sofern die Zustandsmenge des LTS endlich ist, nur mit jeweils endlich vielen Verzweigungen an jedem Knoten. Genauer: Sei s der ausgewählte Zustand. Dann bildet s die Wurzel des Baums und die Äste bestehen aus allen Pfaden σ mit $\sigma_0 = s$, wobei gleiche Präfixe zu einem einzigen Weg (im graphentheorischen Sinn) kollabieren, dh. Verzweigungen treten genau in den Zuständen auf, die der letzte eines gemeinsamen Präfixes von mind. zwei Pfaden sind.

Auch wenn es in den obigen Definitionen nicht gefordert war, werden wir im folgenden von zustandsendlichen Systemen ausgehen. Dies beschränkt jedoch wie gesagt nicht die Länge von Pfaden.

hier sollte ein Bild sein

2 Logiken

Wir stellen i.W. zwei[1] temporale Logiken vor, in denen Eigenschaften von Modellen ausdrückbar sind: CTL (Computation Tree Logic) und μM (modaler μ-Kalkül). Letzterer ist ausdrucksstärker als CTL, dh. man kann darin mehr Modelle unterscheiden. Mit CTL werden wir uns eingehender befassen und auch einige Beweise führen, da das (hoffentlich) eine recht gute Hinführung auf μM darstellt.

2.1 CTL

Die Modelle für CTL und die erweiterte Logik CTL* - auf die wir aber nur kurz hinweisen werden - sind Berechnungsbäume, denen die Logik ihren Namen verdankt.

Im Gegensatz etwa zur Linearen Temporalen Logik LTL handelt es sich hier um eine verzweigende Logik[2].

Die den Berechnungsbäumen zugrundeliegenden („aufgefaltete“) Zustandsübergangssysteme sind endliche knotenbeschriftete Graphen, bei denen außerdem davon ausgegangen wird, daß *jeder Zustand einen Nachfolger hat*; die jeweilige Übergangsrelation δ also linkstotal ist. Das bedeutet, daß die (endlich vielen) Äste der Berechnungsbäume alle unendlich lang sind und damit auch die Pfade von Zuständen, über die durch CTL-Formeln Aussagen formuliert werden. Nichtsdestotrotz kann es aber Pfade geben, auf denen (irgendwann) immer wieder nur derselbe Zustand sich selbst nachfolgt. Wenn im folgenden von einem Modell M die Rede ist, dann ist ein solcher Berechnungsbaum gemeint.

2.1.1 Syntax & Semantik

CTL-Syntax

Sei P eine Menge von atomaren logischen Aussagen (Propositionen). Die Menge Φ von wohlgeformten CTL-Formeln ist:

- $P \subseteq \Phi$
- ist $\varphi \in \Phi$, so ist auch $\neg\varphi \in \Phi$
- sind $\varphi, \psi \in \Phi$, so ist auch $\varphi \wedge \psi \in \Phi$
- ist $\varphi \in \Phi$, so sind auch EX φ, EG $\varphi \in \Phi$
- sind $\varphi, \psi \in \Phi$, so ist auch φ EU $\psi \in \Phi$

Die übrigen aussagenlogischen Operatoren werden in der üblichen Weise als Abkürzungen definiert, also $\varphi \vee \psi$ für $\neg(\neg\varphi \wedge \neg\psi)$, $\varphi \to \psi$ für $\neg\varphi \vee \psi$, $\varphi \leftrightarrow \psi$ für $\varphi \to \psi \wedge \psi \to \varphi$, etc.; ebenso wie die booleschen Konstanten: $\mathbf{tt}$ für $\neg\,\mathbf{ff}$ und $\mathbf{ff}$ für $p \wedge \neg p$ mit beliebigem $p \in P$ (wir setzen $P \neq \emptyset$ voraus).

Die temporalen Operatoren setzen sich zusammen aus einem Quantor *über Pfade* (Pfadquantor; E für existenzielle und A für universelle Quantifizierung) *gefolgt von* einem

[1] eigentlich noch: CTL* und die Hennessy-Milner-Logik; auf die erste wird jedoch nur hingewiesen und die zweite ist syntaktisch in μM enthalten.

[2] Eine generelle Gegenüberstellung verschiedener Modal- und Temporallogiken (und eine Axiomatisierung von CTL*) findet sich in [St89].

Quantor *über Zustände* auf einem Pfad (Zustandsquantor; F für existenzielle und G für universelle Quantifizierung, X für den Nachfolgezustand, U für starke Präzedenz[3], W für schwache Präzedenz).

Diese Einschränkung wird in der erweiterten Logik CTL* fallengelassen, in deren Formeln beliebige Quantoren aufeinanderfolgen dürfen. Allerdings muß dann unterschieden werden zwischen *Zustands*formeln, die bezüglich eines Zustands (und nichts weiter) interpretierbar sind und *Pfad*formeln andererseits, die nur interpretierbar sind bezüglich eines (bestimmten) Pfades *und* eines Zustandes darauf. Die wohlgeformten Formeln von CTL* sind eingeschränkt auf solche, die entweder gar keinen oder als äußersten Quantor einen Pfadquantor enthalten, mithin auf Zustandsformeln.
Die Zustandsquantoren F, G, X, U und W entsprechen den LTL-Operatoren $\Diamond$ (sometime), $\Box$ (always), $\circ$(next), until bzw. waits-for (auch: unless). Der besseren Lesbarkeit halber werden für CTL*-Formeln häufig $\exists$ und $\forall$ als Pfadquantoren und die LTL-Operatoren zur Quantifizierung über Zustände verwendet. Beispielsweise ist $\exists\Box\Diamond\phi$ eine wohlgeformte CTL*-Formel, die in CTL nicht ausdrückbar ist. Auf dieses Beispiel werden wir später zurückkommen.

Bevor die formale Semantik von CTL-Formeln gegeben wird, erklären wir informell die Bedeutung der obigen drei „offiziellen“ und einiger von ihnen abgeleiteter temporaler Operatoren [4].

EX φ	in einem Nachfolger φ („Exists neXt“)
AX φ	in allen Nachfolgern φ („All neXt“); Abkz. für $\neg$ EX $\neg\varphi$
EG φ	auf einem Pfad immer φ („Exists Globally“)
AF φ	auf allen Pfaden irgendwann φ („All Finally“); Abkz. für $\neg$ EG $\neg\varphi$
φ EU ψ	auf einem Pfad: φ bis irgendwann ψ („Exists Until“)
EF φ	auf einem Pfad irgendwann φ; Abkz. für **tt** EU φ
AG φ	auf allen Pfaden immer φ; Abkz. für $\neg$ EF $\neg\varphi$
φ EW ψ	auf einem Pfad: φ solange bis ψ („Exists Waits-for“, schwaches until, unless); Abkz. für (φ EU ψ) $\vee$ EG φ
φ AW ψ	auf allen Pfaden: φ solange bis ψ Abkz. für $\neg(\neg\psi$ EU $(\neg\varphi \wedge \neg\psi))$
φ AU ψ	auf allen Pfaden: φ bis irgendwann ψ Abkz. für $\neg(\neg\psi$ EW $(\neg\varphi \wedge \neg\psi))$ oder einfacher: (φ AW ψ) $\wedge$ AF ψ

Daß die letzten beiden Operatoren tatsächlich die intendierte Semantik haben, ist nicht unbedingt offensichtlich. Für einen Beweis benötigen wir zunächst die Semantik der Basisoperatoren, die induktiv nach der Struktur der Formeln definiert wird.

CTL-Semantik
Seien $p \in P$ eine atomare und φ, ψ beliebige CTL-Formeln.

[3] gemeint ist hier eine Präzedenz im *zeitlichen* Sinne, nicht etwa i.S. der Präzedenz von Operatoren

[4] es lassen sich natürlich noch andere definieren, z.B. findet sich in der Literatur ein Quantor # über Zustände für „fast immer“.

$M, s \models p$	gdw.	$p \in l(s)$ (für $p \in P$)
$M, s \models \neg\varphi$	gdw.	$M, s \not\models \varphi$
$M, s \models \varphi \wedge \psi$	gdw.	$M, s \models \varphi$ und $M, s \models \psi$
$M, s \models \text{EX } \varphi$	gdw.	es ex. ein $t \in S$, sd. $(s, t) \in \delta$ und $M, t \models \varphi$
$M, s \models \text{EG } \varphi$	gdw.	es ex. ein Pfad σ in M mit $\sigma_0 = s$ und f.a. $i \in \mathbf{N} : M, \sigma_i \models \varphi$
$M, s \models \varphi \text{ EU } \psi$	gdw.	es ex. ein Pfad σ in M mit $\sigma_0 = s$ und ein $i \in \mathbf{N}$, sd. $M, \sigma_i \models \psi$ und f.a. $j < i : M, \sigma_j \models \varphi$

Damit folgt für die abgeleiteten CTL-Operatoren:

$M, s \models \text{AX } \varphi$	$\Leftrightarrow$	für alle $t \in S : (s, t) \in \delta \Longrightarrow M, t \models \varphi$
$M, s \models \text{AF } \varphi$	$\Leftrightarrow$	f.a. Pfade σ in M mit $\sigma_0 = s$ existiert ein $i \in \mathbf{N}$, sd. $M, \sigma_i \models \varphi$
$M, s \models \text{EF } \varphi$	$\Leftrightarrow$	es ex. ein Pfad σ in M mit $\sigma_0 = s$ und ein $i \in \mathbf{N}$, sd. $M, \sigma_i \models \varphi$
$M, s \models \text{AG } \varphi$	$\Leftrightarrow$	f.a. Pfade σ in M mit $\sigma_0 = s$ und f.a. $i \in \mathbf{N}$ gilt: $M, \sigma_i \models \varphi$
$M, s \models \varphi \text{ EW } \psi$	$\Leftrightarrow$	es ex. ein Pfad σ in M mit $\sigma_0 = s$, sd.: f.a. $i \in \mathbf{N} : M, \sigma_i \models \varphi$ oder es ex. $i \in \mathbf{N}$ sd. $M, \sigma_i \models \psi$ und f.a. $j < i : M, \sigma_j \models \varphi$
$M, s \models \varphi \text{ AW } \psi$	$\Leftrightarrow$	f.a. Pfade σ in M mit $\sigma_0 = s$ gilt: f.a. $i \in \mathbf{N} : M, \sigma_i \models \varphi$ oder es ex. $i \in \mathbf{N}$, sd. $M, \sigma_i \models \psi$ und f.a. $j < i : M, \sigma_j \models \varphi$
$M, s \models \varphi \text{ AU } \psi$	$\Leftrightarrow$	f.a. Pfade σ in M mit $\sigma_0 = s$ existiert ein $i \in \mathbf{N}$, sd. $M, \sigma_i \models \psi$ und f.a. $j < i : M, \sigma_j \models \varphi$

2.1.2 Interdefinierbarkeit von U und W

Zum Beweis[5] der Semantik von AW und AU wird zunächst die Interdefinierbarkeit der (CTL*-) Operatoren U und W gezeigt, die den LTL-Operatoren **until** bzw. **waits-for** entsprechen. In Kombination mit den Pfadquantoren A und E ergeben sich dann die Behauptungen. Dabei argumentieren wir „rückwärts“, dh. die Semantik (aller) binären temporalen Operatoren wird angenommen, um die jeweilige semantische Äquivalenz zu der entsprechenden Abkürzung wie oben angegeben zu zeigen.

Interdefinierbarkeit von until und waits-for

Für die Menge Σ aller (einseitig beschränkten) Pfade in M und die Menge Φ_{LTL} aller LTL-Formeln (das sind in CTL* die Formeln, die keinen Pfadquantor enthalten), definieren wir die Hilfsfunktion

$$\begin{aligned} min: \quad & \Sigma \times \Phi_{LTL} \to \mathbb{N} \cup \{\infty\} \\ (\sigma, \varphi) \mapsto \quad & \begin{cases} \infty \text{ falls f.a. } i \in \mathbb{N} : \sigma_i \not\models \varphi \\ min(\{\, i \in \mathbb{N} \mid \sigma_i \models \varphi \,\}) \text{ sonst} \end{cases} \end{aligned}$$

[5] die letzte Liste enthält Behauptungen, keine Definitionen

wobei natürlich $min : 2^N \to \mathbb{N}$ die naheliegende Minimumfunktion auf Mengen von natürlichen Zahlen ist[6].

Was läßt sich nun etwa aus $min(\sigma,\varphi) < min(\sigma,\psi)$ folgern?
Wegen der Ungleichheit zunächst $min(\sigma,\varphi) \in \mathbb{N}$, dh. daß auf σ irgendwann einmal φ eintritt, also ein kleinstes $i \in \mathbf{N}$ existiert, sd. $\sigma_i \models \varphi$. Weiterhin: bis einschließlich σ_i gilt *nicht* ψ. Daraus folgt insbesondere, daß es einen Zustand gibt, in dem zum ersten Mal φ der Fall ist und $\neg\psi$, nämlich σ_i. Es gilt also:

$$\begin{array}{ll} & min(\sigma,\varphi) < min(\sigma,\psi) \\ \Leftrightarrow & \text{auf } \sigma\text{: } \varphi \text{ tritt irgendwann ein und zwar } \textit{bevor } \psi \text{ eintritt} \\ & \text{(was } \textit{nicht ausschließt}\text{, daß } \psi \text{ niemals eintritt)} \\ \Leftrightarrow & \text{es ex. } i \in \mathbf{N} : \sigma_i \models \varphi \wedge \neg\psi \text{ und f.a.} j < i : \sigma_j \models \neg\psi \\ \Leftrightarrow & \sigma_0 \models \neg\psi \text{ U } (\varphi \wedge \neg\psi) \end{array}$$

Anmerkung: $\neg\psi$ U $(\varphi \wedge \neg\psi)$ ist äquivalent zu $(\neg\varphi \wedge \neg\psi)$ U $(\varphi \wedge \neg\psi)$, denn gdw. es ein $i \in \mathbf{N}$ gibt, sd. $\sigma_i \models \varphi$, gibt es auch ein *kleinstes* $i \in \mathbf{N}$, sd. $\sigma_i \models \varphi$; ist i jedoch minimal, dann gilt f.a. $j < i : \sigma_j \models \neg\varphi$.

Betrachte nun:

$$\begin{array}{ll} & min(\sigma,\psi) \leq min(\sigma,\neg\varphi) \\ \Leftrightarrow & \neg(\underbrace{min(\sigma,\neg\varphi) < min(\sigma,\psi)}_{\text{wie oben, nur } \neg\varphi \text{ anstatt } \varphi}) \\ \Leftrightarrow & \sigma_0 \models \neg(\neg\psi \text{ U } (\neg\varphi \wedge \neg\psi)) \end{array}$$

Da andererseits auch

$$\begin{array}{ll} & min(\sigma,\psi) \leq min(\sigma,\neg\varphi) \\ \Leftrightarrow & \text{auf } \sigma\text{: } \neg\varphi \text{ tritt nicht früher ein als } \psi \\ \Leftrightarrow & \text{f.a. } j < min(\sigma,\psi) : \sigma_j \not\models \neg\varphi \\ \Leftrightarrow & \text{f.a. } j < min(\sigma,\psi) : \sigma_j \models \varphi \\ \Leftrightarrow & \text{f.a. } j \in \mathbf{N} : \sigma_j \models \varphi \quad \text{(entspricht dem Fall } min(\sigma,\psi) = \infty) \\ & \text{oder} \\ & \text{es ex. } i \in \mathbf{N},\ \text{sd. } \sigma_i \models \psi \text{ und f.a. } j < i : \sigma_j \models \varphi \quad \text{(entspr. } min(\sigma,\psi) \in \mathbf{N}) \\ \Leftrightarrow & \sigma_0 \models \varphi \text{ W } \psi \end{array}$$

folgt (endlich)

$$\varphi \text{ W } \psi \quad \equiv \quad \neg(\neg\psi \ \text{ U } \ (\neg\varphi \wedge \neg\psi))$$

Umgekehrt gilt auch

$$\varphi \ \text{ U } \ \psi \quad \equiv \quad \neg(\neg\psi \text{ W } (\neg\varphi \wedge \neg\psi))$$

[6] ganz genau: sie liefert $\perp$ aus dem Verband $(L, \leq)$ wobei $L \subseteq \mathbb{N}$

denn

$$\begin{array}{rcll}
\varphi \text{ W } \psi & \equiv & \neg(\neg\psi \text{ U } (\neg\varphi \wedge \neg\psi)) & \mid \text{ setze } x :\equiv \neg\psi \\
\neg(\varphi \text{ W } \neg x) & \equiv & x \text{ U } (\neg\varphi \wedge x) & \\
\neg(\varphi \text{ W } (\neg x \wedge \mathbf{tt})) & \equiv & x \text{ U } (\neg\varphi \wedge x) & \mid \text{ setze } y :\equiv (\neg\varphi \wedge x) \\
\neg(\varphi \text{ W } (\neg x \wedge (y \vee \neg y))) & \equiv & x \text{ U } y & \\
\neg(\varphi \text{ W } (\neg x \wedge y \vee \neg x \wedge \neg y)) & \equiv & x \text{ U } y & \\
\neg(\varphi \text{ W } (\neg x \wedge \neg\varphi \wedge x \vee \neg x \wedge \neg y)) & \equiv & x \text{ U } y & \mid y \equiv (\neg\varphi \wedge x) \\
\neg(\varphi \text{ W } (\neg x \wedge \neg y)) & \equiv & x \text{ U } y & \\
\neg((\varphi \vee \psi) \text{ W } (\neg x \wedge \neg y)) & \equiv & x \text{ U } y & \mid \text{ Semantik von W} \\
\neg(\neg y \text{ W } (\neg x \wedge \neg y)) & \equiv & x \text{ U } y & \mid \neg y \equiv \neg(\neg\varphi \wedge \neg\psi) \equiv \varphi \vee \psi
\end{array}$$

Mit der bekannten Interdefinierbarkeit von All- und Existenzquantor[7] ergibt sich damit (in CTL*):

$$\begin{array}{rcl}
\text{A } (\varphi \text{ W } \psi) & \equiv & \neg \text{ E } (\neg\psi \text{ U } (\neg\varphi \wedge \neg\psi)) \\
\text{E } (\varphi \text{ W } \psi) & \equiv & \neg \text{ A } (\neg\psi \text{ U } (\neg\varphi \wedge \neg\psi)) \\
\text{A } (\varphi \text{ U } \psi) & \equiv & \neg \text{ E } (\neg\psi \text{ W } (\neg\varphi \wedge \neg\psi)) \\
\text{E } (\varphi \text{ U } \psi) & \equiv & \neg \text{ A } (\neg\psi \text{ W } (\neg\varphi \wedge \neg\psi))
\end{array}$$

bzw. gleichbedeutend (in CTL):

$$\begin{array}{rcl}
(\varphi \text{ AW } \psi) & \equiv & \neg(\neg\psi \text{ EU } (\neg\varphi \wedge \neg\psi)) \\
(\varphi \text{ EW } \psi) & \equiv & \neg(\neg\psi \text{ AU } (\neg\varphi \wedge \neg\psi)) \\
(\varphi \text{ AU } \psi) & \equiv & \neg(\neg\psi \text{ EW } (\neg\varphi \wedge \neg\psi)) \\
(\varphi \text{ EU } \psi) & \equiv & \neg(\neg\psi \text{ AW } (\neg\varphi \wedge \neg\psi))
\end{array}$$

2.1.3 Erfüllungsmengen

Gegeben ein Modell M und eine CTL-Formel φ, interessiert man sich u.U. nicht nur dafür, ob φ *überhaupt* in irgendeinem Zustand von M gilt, sondern fragt möglicherweise, *in welchen* Zuständen dies der Fall sei. So kann man - unter adäquater Abstraktion - ein Soft- oder Hardwaresystem als LTS modellieren, um bestimmte Eigenschaften dieses Modells nachzuweisen wie etwa, ob gewisse Fairness- oder Safetybedingungen[8] erfüllt sind, wobei natürlich die Bedingungen bzw. Eigenschaften in einer temporalen Logik wie CTL formuliert sind.

Ausgehend von einer Menge von Anfangszuständen, stellt sich z.B. die Frage, ob Zustände des Modells, die unerwünschte Zustände des modellierten Systems repräsentieren, erreichbar sind oder nicht. Und falls sie es sind, unter welchen Umständen.

Dazu definieren wir bezüglich eines Modells M die **Erfüllungsmenge** $\|\varphi\|_M$ einer CTL-Formel φ als die Menge der Zustände des Modells, in denen φ erfüllt ist:

$$\|\varphi\|_M \quad := \quad \{s \in S \mid M, s \models \varphi\}$$

[7] $\forall\varphi \equiv \neg\exists\neg\varphi$ bzw. $\exists\varphi \equiv \neg\forall\neg\varphi$ oder à la CTL*: A $\varphi \equiv \neg$E$\neg\varphi$ bzw. E $\varphi \equiv \neg$A$\neg\varphi$

[8] nach Leslie Lamport sind Safetybedingungen solche, die sagen daß „nichts Böses“ geschieht

Wie gewohnt wird das Subskript weggelassen, falls das Modell klar ist.

Wenn wir nun noch die Gültigkeit einer Formel in einem Modell M mit den Anfangszuständen $I \subseteq S$ (I von „Initialzustände") definieren als:

$$M \models \varphi \quad :\Leftrightarrow \quad \text{f.a. } i \in I : M, i \models \varphi$$

- also mit ihrer Gültigkeit in allen Anfangszuständen identifizieren, dann läßt sich die obige Frage nach der Eigenschaft φ von M formal so formulieren:

$$M \overset{?}{\models} \varphi \quad \Leftrightarrow \quad I \overset{?}{\subseteq} \|\varphi\|$$

Dies ist das sogenannte Modelchecking-Problem.

Verschiedene Ansätze zur Lösung dieses Problems sind möglich und zwei werden wir hier vorstellen. Andere, wie die Reduktion auf das Lösen eines Bool'schen Gleichungssystems wurden bereits im Seminar vorgetragen. Der naheliegende „Ansatz" - nämlich für alle $i \in I$ zu prüfen, ob $i \in \|\varphi\|$ - ist eigentlich keiner, denn er adressiert nicht das Problem, herauszufinden ob in einem bestimmten Zustand eine bestimmte Formel nun gilt oder nicht (die abschließende Prüfung der Inklusionsbeziehung zweier Mengen bzw. der Leerheitstest einer Schnittmenge ist dann „nicht mehr so wild").

Im folgenden werden wir Charakterisierungen von Erfüllungsmengen entwickeln, die sich auf δ, Mengenoperationen und Fixpunktausdrücke stützen. Eine kompakte Repräsentation von Zustandsmengen, Formeln und δ vorausgesetzt ermöglichen diese Charakterisierungen eine effiziente Berechnung von Erfüllungsmengen.

Wir definieren zunächst die Funktionen $\delta_\exists^{-1}$ und $\delta_\forall^{-1}$, die Mengen von Zuständen auf best. Mengen von deren Vorgängern bzgl. δ abbilden.

$$\begin{aligned} \delta_\exists^{-1} :\ & 2^S \to 2^S \\ T \mapsto\ & \{\, s \in S \mid \text{es ex. } t \in T, sd.(s,t) \in \delta \,\} \end{aligned}$$

$$\begin{aligned} \delta_\forall^{-1} :\ & 2^S \to 2^S \\ T \mapsto\ & \{\, s \in S \mid \text{f.a. } t \in S : (s,t) \in \delta \Rightarrow t \in T \,\} \end{aligned}$$

$\delta_\exists^{-1}(\,T\,)$ ist also die Menge von Zuständen, die mind. einen Nachfolger in T haben, dh. die Menge aller Vorgänger von Zuständen in T.
$\delta_\forall^{-1}(\,T\,)$ ist die Menge von Zuständen, deren Nachfolger allesamt in T liegen. Beachte: Zustände die *gar keinen* Nachfolgern haben, sind immer in $\delta_\forall^{-1}(\,T\,)$ enthalten, für alle $T \subseteq S$.
Desweiteren schreiben wir abkürzend $\delta(s)$ für $\{\, t \in S \mid (s,t) \in \delta \,\}$ die Menge der Nachfolger eines Zustandes s. So ist z.B. für alle $T \subseteq S$:

$$\begin{aligned} \delta_\forall^{-1}(\,T\,) &= \{\, s \in S \mid \delta(s) \subseteq T \,\} \\ \delta_\exists^{-1}(\,T\,) &= \{\, s \in S \mid \delta(s) \cap T \neq \emptyset \,\} \end{aligned}$$

Außerdem werden wir etwas salopp von der Erfüllungsmenge eines Operators O sprechen. Damit ist gemeint: die Erfüllungsmenge von Formeln, deren Hauptoperator, dh. der erste auszuwertende Operator O ist, wobei die Auswertungsreihenfolge zuerst durch

Klammerung, dann durch Operatorpräzedenz und schließlich als vlnr. festgelegt ist. Atomare Formeln (Propositionen) werden als nullstellige Operatoren betrachtet.

Die Erfüllungsmengen der einfachen CTL-Basisoperatoren sind offensichtlich:

$$\begin{array}{rcll} \|p\| &=& \{\, s \in S \mid p \in l(s) \,\} & \quad (p \in P \text{ Proposition, } l \text{ Labelling-Funktion}) \\ \|\neg\varphi\| &=& S \setminus \|\varphi\| & \\ \|\varphi \wedge \psi\| &=& \|\varphi\| \cap \|\psi\| & \\ \|\mathrm{EX}\,\varphi\| &=& \delta_{\exists}^{-1}(\,\|\varphi\|\,) & \end{array}$$

Bevor wir zu den noch fehlenden Basisoperatoren EG und EU übergehen, hier noch die einfachen abgeleiteten Operatoren, deren Erfüllungsmengen natürlich auch mit dem obigen schon formulierbar wären, mit Hinblick auf effiziente Berechnung aber vielleicht besser wie folgt implementiert werden:

$$\begin{array}{rcl} \|\mathbf{ff}\,\| &=& \emptyset \qquad (\text{ i.e.: } \bot \text{ von } (2^S, \subseteq)\ ) \\ \|\mathbf{tt}\,\| &=& S \qquad (\text{ i.e.: } \top \text{ von } (2^S, \subseteq)\ ) \\ \|\varphi \vee \psi\| &=& \|\varphi\| \cup \|\psi\| \\ \|\varphi \to \psi\| &=& S \setminus \|\varphi\| \cup \|\psi\| \\ \|\varphi \leftrightarrow \psi\| &=& (S \setminus \|\varphi\| \cup \|\psi\|) \cap (S \setminus \|\psi\| \cup \|\varphi\|) \\ &=& \underbrace{S \setminus \|\varphi\| \cap S \setminus \|\psi\|}_{=S\setminus(\|\varphi\|\cup\|\psi\|)} \cup \underbrace{\underbrace{S \setminus \|\varphi\| \cap \|\varphi\|}_{=S\setminus\|\varphi\|} \cup \underbrace{S \setminus \|\psi\| \cap \|\psi\|}_{S\setminus\|\psi\|}}_{=S\setminus(\|\varphi\|\cup\|\psi\|)} \cup \|\psi\| \cap \|\varphi\| \\ &=& S \setminus (\|\varphi\| \cup \|\psi\|) \ \cup\ \|\psi\| \cap \|\varphi\| \\ (&=& \|\neg\varphi \wedge \neg\psi \ \vee\ \varphi \wedge \psi\| \quad) \\ \|\mathrm{AX}\,\varphi\| &=& \delta_{\forall}^{-1}(\,\|\varphi\|\,) \end{array}$$

2.1.4 Fixpunktcharakterisierungen

Fixpunktcharakterisierung von $\|\mathrm{EG}\ \varphi\|$
Offensichtlich gilt die rekursive Beziehung[9]

$$\mathrm{EG}\ \varphi \quad \Leftrightarrow \quad \varphi \ \wedge\ \mathrm{EX}\ (\mathrm{EG}\ \varphi\,)$$

also auf semantischer Ebene

$$\|\mathrm{EG}\ \varphi\| \quad = \quad \|\varphi\| \ \cap\ \delta_{\exists}^{-1}(\,\|\mathrm{EG}\ \varphi\|\,) \tag{1}$$

dh. $\|\mathrm{EG}\ \varphi\|$ ist die Menge der Vorgänger von Zuständen, in denen (dann wieder) EG φ gilt, *beschränkt* auf diejenigen (Vorgänger), in denen φ selbst (schon) gilt.

Bezüglich der Funktion

$$\begin{array}{rl} \xi: & 2^S \to 2^S \\ T \mapsto & \|\varphi\| \ \cap\ \delta_{\exists}^{-1}(\,T\,) \end{array}$$

[9] die rechte Seite nennt man Auffaltung (unfolding) der linken Seite

die die Zustände T auf die T-Vorgänger abbildet, *beschränkt* auf diejenigen Vorgänger, in denen φ gilt,

ist $\|\text{EG } \varphi\|$ **ein Fixpunkt von** ξ, denn

$$\begin{aligned} \xi(\|\text{EG } \varphi\|) &= \|\varphi\| \;\cap\; \delta_\exists^{-1}(\,\|\text{EG } \varphi\|\,) \\ &= \|\text{EG } \varphi\| \end{aligned}$$

Das ist wenig verwunderlich, denn wir haben ξ ja nach dem Vorbild der Gleichung (1) „gebaut“, die wir als selbstverständlich genommen hatten und deren syntaktisches Äquivalent als offensichtlich apostrophiert wurde. Genaugenommen müssten auch diese bewiesen werden, was wir dieses eine Mal noch etwas ausführen, um den Weg der Argumentation (über „Sem. EG“) zu illustrieren:

$$\begin{aligned} \xi(\|\text{EG } \varphi\|) &= \|\varphi\| \;\cap\; \delta_\exists^{-1}(\,\|\text{EG } \varphi\|\,) \\ &= \{\, s \in S \mid s \models \varphi \;\wedge\; s \models \text{EX (EG } \varphi)\,\} && (\text{ Def. } \|\;\|\,, \delta_\exists^{-1}\ ) \\ &= \{\, s \in S \mid s \models \text{EG } \varphi\,\} && (\text{ Sem. EG }) \\ &= \|\text{EG } \varphi\| && (\text{ Def. } \|\;\|\ ) \end{aligned}$$

Außerdem ist $\|\text{EG } \varphi\|$ der größte[10] Fixpunkt von ξ, denn:

Sei F beliebiger Fixpunkt von ξ und $s_0 \in F$ ebenfalls beliebig.
Dann ist sowohl $s_0 \in \|\varphi\|$, also $s_0 \models \varphi$ als auch $s_0 \in \delta_\exists^{-1}(\,F\,)$, mithin ex. $s_1 \in F$, sd. $s_1 \in \delta(s_0)$, dh. s_0 hat (mind.) einen Nachfolger s_1 in F. Für diesen gilt wiederum: $s_1 \models \varphi$ und daß er einen Nachfolger $s_2 \in F$ hat, usw.
Da s_0 beliebig gewählt war, gilt für alle Zustände $s \in F$: es ex. ein Pfad σ mit $s = \sigma_0$, dessen Zustände allesamt in F liegen (f.a. $i \in \mathbb{N} : \sigma_i \in F$) und in all diesen gilt φ (f.a. $i \in \mathbb{N} : \sigma_i \models \varphi$). Also gilt f.a. $s \in F : s \models \text{EG } \varphi$. Daraus folgt: $F \subseteq \|\text{EG } \varphi\|$. Wegen der beliebigen Wahl von F ist *jeder* Fixpunkt von ξ in $\|\text{EG } \varphi\|$ enthalten, und also ist $\|\text{EG } \varphi\| = \nu T.\xi(T)$.

$\square$

Fixpunktcharakterisierung von $\|\varphi \text{ EU } \psi\|$
Wie vorher wird die Formel „aufgefaltet“:

$$\begin{aligned} \varphi \text{ EU } \psi &\;\Leftrightarrow\; \psi \;\vee\; (\,\varphi \;\wedge\; \text{EX } (\varphi \text{ EU } \psi)\,) \\ \|\varphi \text{ EU } \psi\| &\;=\; \|\psi\| \;\cup\; (\,\|\varphi\| \;\cap\; \delta_\exists^{-1}(\,\|\varphi \text{ EU } \psi\|\,)\,) \end{aligned}$$

Behauptung: $\|\varphi \text{ EU } \psi\|$ ist **kleinster Fixpunkt** von

$$\begin{aligned} \zeta : &\quad 2^S \to 2^S \\ T \mapsto &\quad \|\psi\| \;\cup\; (\,\|\varphi\| \;\cap\; \delta_\exists^{-1}(\,T\,)\,) \end{aligned}$$

<u>Beweis:</u>

[10] selbstverständlich bzgl. der partiellen Ordnung $\subseteq$

- $\|\varphi \text{ EU } \psi\|$ ist ein Fixpunkt: klar.
- Sei F beliebiger Fixpunkt von ζ. Dann bleibt zu zeigen: $\|\varphi \text{ EU } \psi\| \subseteq F$.

  Zunächst: $F = \|\psi\| \;\cup\; \|\varphi\| \cap \delta_\exists^{-1}(\,F\,)$ also $\|\varphi\| \cap \delta_\exists^{-1}(\,F\,) \subseteq F$, und mithin gilt f.a. $s \in S : s \models \varphi \;\wedge\; s \in \delta_\exists^{-1}(\,F\,) \;\Rightarrow\; s \in F$,
  dh.: jeder Zustand, der φ erfüllt und einen Nachfolger in F hat, ist selbst in F.

  Sei nun $s \in \|\varphi \text{ EU } \psi\|$ beliebig. Dann ex. ein Pfad σ mit $\sigma_0 = s$ und ein $i \in \mathbb{N}$, sd. $\sigma_i \models \psi$ und f.a. $j < i : \sigma_j \models \varphi$.
  Insbesondere: $i \geq 1 \;\Rightarrow\; s \models \varphi$

  Induktion über i:
  $\underline{i = 0:}$ Dann $s \models \psi \;\Rightarrow\; s \in \|\psi\| \;\Rightarrow\; s \in F$
  $\underline{i \to i+1:}$ Die I.V. besagt: f.a. $1 \leq j \leq i : \sigma_j \in F$.
  Es gilt: $s \models \varphi$ und $s = \sigma_0 \in \delta_\exists^{-1}(\,\{\sigma_1\}\,)$ und nach I.V. $\sigma_1 \in F \;\Rightarrow\; s \in F$,
  dh.: s erfüllt φ und hat nach I.V. einen Nachfolger in F.
  Weil aber F ein Fixpunkt ist (s.o.), folgt daraus $s \in F$.
- Insgesamt (wg. der beliebigen Wahl von F und s) ergibt sich: $\|\varphi \text{ EU } \psi\|$ ist in jedem Fixpunkt von ζ enthalten. Weil $\|\varphi \text{ EU } \psi\|$ auch selbst ein Fixpunkt von ζ ist[11], folgt daher: $\|\varphi \text{ EU } \psi\| = \mu T.\zeta(T)$.

$\square$

Bei der Fixpunktcharakterisierung von EG haben wir die Induktion über die Pfadlänge noch hinter einem „usw.“ versteckt. Hier jedoch ist sie explizit und es sei noch eine Bemerkung dazu gestattet: Die Basis ist σ_i (und nicht etwa σ_0), will meinen: wir blicken sozusagen von σ_i (der ψ erfüllt und damit offensichtlich in F liegt) *zurück* und „hängen“ im Induktionsschritt immer noch einen φ-erfüllenden Vorgänger „dran“.
Das ist insofern interessant, als diese Argumentation für

$$\begin{aligned} \|\varphi \text{ EW } \psi\| &= \|\text{EG } \varphi \vee (\varphi \text{ EU } \psi)\| \\ &= \|\text{EG } \varphi\| \cup \|\varphi \text{ EU } \psi\| \\ \Rightarrow\; \|\varphi \text{ EU } \psi\| \subseteq \|\varphi \text{ EW } \psi\| & \end{aligned}$$

nicht mehr funktioniert, jedoch (erstaunlicherweise?) $\|\varphi \text{ EW } \psi\| = \nu T.\zeta(T)$. Bevor wir dies verifizieren, betrachten wir noch eine Folgerung aus dem eben Bewiesenen.

Fixpunktcharakterisierung von $\|\text{EF } \psi\|$
EF ψ war als Abkürzung für $\mathbf{tt}$ EU ψ definiert worden. Wenn man also in der Definition von ζ jedes Vorkommen von φ durch $\mathbf{tt}$ ersetzt

$$\begin{aligned} \zeta' : &\quad 2^S \to 2^S \\ T \mapsto &\quad \|\psi\| \;\cup\; (\,\|\mathbf{tt}\| \;\cap\; \delta_\exists^{-1}(\,T\,)\,) \\ = &\quad \|\psi\| \;\cup\; (\,S \;\cap\; \delta_\exists^{-1}(\,T\,)\,) \\ = &\quad \|\psi\| \;\cup\; \delta_\exists^{-1}(\,T\,) \end{aligned}$$

[11] Zwischenfrage(n): hinreichende oder/und notwendige Bedingung? Wie heißen die Zustandsmengen, die keine Fixpunkte sind, mit denen aber Teil 2 des Beweises noch einwandfrei funktioniert?

erhält man diejenige Funktion, deren kleinster Fixpunkt die Erfüllungsmenge von EF ψ ist:

$$\|\text{EF } \psi\| \quad = \quad \mu T.\, \|\psi\| \,\cup\, \delta_{\exists}^{-1}(\,T\,)$$

Fixpunktcharakterisierung von $\|\varphi \text{ EW } \psi\|$
Zu zeigen ist:

$$\|\varphi \text{ EW } \psi\| \quad = \quad \nu T.\, \|\psi\| \,\cup\, (\,\|\varphi\| \,\cap\, \delta_{\exists}^{-1}(\,T\,)\,)$$

- $\|\varphi \text{ EW } \psi\|$ ist ein Fixpunkt: klar.
- Da es sich um einen größten Fixpunkt handelt (handeln soll), müssen wir diesmal zeigen: $F \subseteq \|\varphi \text{ EW } \psi\|$ mit F beliebiger Fixpunkt von ζ.
  Wie schon gesehen, trifft dies zumindest für $\mu T.\zeta(T) = \|\varphi \text{ EU } \psi\|$ zu.
  Sei $s \in F$ beliebig. Falls $s \in \|\varphi \text{ EU } \psi\| \;\Rightarrow\; s \in \|\varphi \text{ EW } \psi\|$
  Andernfalls gilt zumindest wie oben: $s \models \varphi \wedge s \in \delta_{\exists}^{-1}(\,F\,)$, s erfüllt also φ und hat einen Nachfolger t in F. Wenn aber $s \notin \|\varphi \text{ EU } \psi\|$, dann muß auch $t \notin \|\varphi \text{ EU } \psi\|$ (andernfalls wäre eben auch $s \in \|\varphi \text{ EU } \psi\|$). Für t und alle dessen direkten und indirekten Nachfolger gilt aber genau dasselbe wie für s: alle erfüllen φ, aber keiner hat einen Nachfolger, der ψ erfüllt. s liegt also auf einem Pfad σ, sd. f.a. $i \in \mathbb{N} : \sigma_i \models \varphi$, mithin $s \in \|\text{EG } \varphi\| \quad \Rightarrow \quad s \in \|\varphi \text{ EW } \psi\|$

$\square$

Eine kompakte Zusammenfassung der Ergebnisse dieses Abschnitts:

$$
\begin{array}{lcccr}
\|\mathbf{tt}\| & = & S & \emptyset & = \|\mathbf{ff}\| \\
\|p\| & = & \{\, s \in S \mid p \in l(s) \,\} & S \setminus \|\varphi\| & = \|\neg\varphi\| \\
\|\varphi \vee \psi\| & = & \|\varphi\| \cup \|\psi\| & \|\varphi\| \cap \|\psi\| & = \|\varphi \wedge \psi\| \\
\\
\|\mathrm{EX}\ \varphi\| & = & \delta_\exists^{-1}(\,\|\varphi\|\,) & \delta_\forall^{-1}(\,\|\varphi\|\,) & = \|\mathrm{AX}\ \varphi\| \\
\\
\|\mathrm{EG}\ \varphi\| & = & \nu T.\, \|\varphi\| \cap \delta_\exists^{-1}(\,T\,) & \nu T.\, \|\varphi\| \cap \delta_\forall^{-1}(\,T\,) & = \|\mathrm{AG}\ \varphi\| \\
\|\mathrm{EF}\ \varphi\| & = & \mu T.\, \|\varphi\| \cup \delta_\exists^{-1}(\,T\,) & \mu T.\, \|\varphi\| \cup \delta_\forall^{-1}(\,T\,) & = \|\mathrm{AF}\ \varphi\| \\
\\
\|\varphi\ \mathrm{EW}\ \psi\| & = & \nu T.\, \|\psi\| \cup (\,\|\varphi\| \cap \delta_\exists^{-1}(\,T\,)\,) & \nu T.\, \|\psi\| \cup (\,\|\varphi\| \cap \delta_\forall^{-1}(\,T\,)\,) & = \|\varphi\ \mathrm{AW}\ \psi\| \\
\|\varphi\ \mathrm{EU}\ \psi\| & = & \mu T.\, \|\psi\| \cup (\,\|\varphi\| \cap \delta_\exists^{-1}(\,T\,)\,) & \mu T.\, \|\psi\| \cup (\,\|\varphi\| \cap \delta_\forall^{-1}(\,T\,)\,) & = \|\varphi\ \mathrm{AU}\ \psi\|
\end{array}
$$

- exist. Pfadquantor E $\rightsquigarrow \delta_\exists^{-1}$
- univ. Pfadquantor A $\rightsquigarrow \delta_\forall^{-1}$
- exist. Zustandsquantor (F, U) $\rightsquigarrow \mu$
- univ. Zustandsquantor (G, W) $\rightsquigarrow \nu$
- $\vee$ vs. $\wedge$ bzw. F vs. G $\rightsquigarrow \cup$ vs. $\cap$
- $\neg \rightsquigarrow \setminus$ bzw. Mengenkomplement
- **tt** vs. **ff** $\rightsquigarrow \top$ vs. $\bot$

2.2 Modallogik mit Fixpunkten

Der modale μ-Kalkül, eine modale Logik mit Operatoren für extremale Fixpunkte, eingeführt von Dexter Kozen [Koz82], ist eine sehr ausdrucksstarke temporale Aussagenlogik zur Beschreibung von Liveness-, Safety- und zyklischen Eigenschaften. Er basiert auf der von Hennessy und Milner in [HM80, HM85] eingeführten modalen Logik zur Verwendung in Verbindung mit einer Prozeßalgebra wie Hoares CSP (Communicating Sequential Processes) oder CCS (Calculus of Communicating Systems). Eine ausführliche Darstellung modaler und temporaler Logiken für Prozesse und Grundlage dieser Arbeit ist [St04].

Anders als dort werden wir markierte Zustandsübergangssysteme direkt als Modelle betrachten, die ansonsten die Semantik von Prozessen darstellen. Sie sind sowohl knoten- als auch kantenbeschriftet und unterliegen nicht mehr der Einschränkung einer linkstotalen Übergangsrelation wie im Falle von CTL*.

2.2.1 Hennessy-Milner-Logik

Wir beginnnen mit der leicht erweiterten Logik von Hennessy/Milner, die weder Propositionen (außer **tt** und **ff**) noch (freie) Variablen noch Fixpunkte kennt, mit der aber Aussagen über die Beschriftungen an den *Kanten* formuliert werden können.

HM-Syntax
Sei also $K \subseteq \mathcal{A}$ eine Menge von Kantenbeschriftungen oder, aus Sicht einer Prozeßalgebra: Aktionen, was kürzer ist und hier synonym verwendet wird. Die Menge Φ der wohlgeformten Formeln ist:

- $\mathbf{tt}, \mathbf{ff} \in \Phi$
- sind $\varphi, \psi \in \Phi$, so ist auch $\varphi \wedge \psi \in \Phi$
- sind $\varphi, \psi \in \Phi$, so ist auch $\varphi \vee \psi \in \Phi$
- $[K] \in \Phi$
- $\langle K \rangle \in \Phi$

Diese Logik ist gegenüber dem Original insofern erweitert, als in ihr Mengen von Aktionen innerhalb der Modalitäten notiert werden anstatt einzelner Aktionen.

Außerdem fällt auf, daß es keine Negation gibt; dazu später mehr.

HM-Semantik
Wie bei CTL geben wir an, wann ein Zustand s in einem Modell M erfüllt:

$M, s \models \mathbf{tt}$
$M, s \not\models \mathbf{ff}$
$M, s \models \varphi \wedge \psi$ gdw. $M, s \models \varphi$ und $M, s \models \psi$
$M, s \models \varphi \vee \psi$ gdw. $M, s \models \varphi$ oder $M, s \models \psi$
$M, s \models [K]\,\varphi$ gdw. f.a. $t \in \{\, t \in S \mid \alpha \in K, (s,t) \in \delta_\alpha \,\}$ gilt: $M, t \models \varphi$
$M, s \models \langle K \rangle\,\varphi$ gdw. es ex. $t \in \{\, t \in S \mid \alpha \in K, (s,t) \in \delta_\alpha \,\}$, sd.: $M, t \models \varphi$

Der Übersichtlichkeit halber werden innerhalb der Modalitäten die Mengenklammern weggelassen, wenn die Menge der Aktionen explizit angegeben wird; also $[\alpha_1, \ldots, \alpha_n]$ anstatt $[\{\alpha_1, \ldots, \alpha_n\}]$ und $\langle \alpha_1, \ldots, \alpha_n \rangle$ anstatt $\langle \{\alpha_1, \ldots, \alpha_n\} \rangle$.
Eine weitere Abkürzung betrifft den Fall, daß bestimmte Aktionen *ausgeschlossen* werden sollen. Wenn also z.B. ausgedrückt werden soll, daß für alle Nachfolger *außer denen, die mit a erreichbar sind* φ gilt, so kann dies durch $[\mathcal{A} \setminus \{a\}]\, \varphi$ geschehen, was mit $[-a]\, \varphi$ abgekürzt wird. Soll sich die Modalität auf das gesamte Alphabet beziehen, wie etwa in $\langle \mathcal{A} \rangle\, \varphi \Leftrightarrow \langle \mathcal{A} \setminus \emptyset \rangle\, \varphi$, so wird dies mit $\langle - \rangle\, \varphi$ abgekürzt.

Welche Eigenschaften können damit nun ausgedrückt werden? Offensichtlich liegt der Fokus auf den Übergängen und nicht den Zuständen des Transitionssystems. Die simple *Möglichkeit* eines a-Übergangs drückt $\langle a \rangle \mathbf{tt}$ aus, dessen *Unmöglichkeit* hingegen $[a]\, \mathbf{ff}$.

Wie gesagt sind auch Zustände ohne irgendeinen Nachfolger möglich; in solchen gilt z.B. $[-]\, \mathbf{ff}$, womit Terminierung bzw. ein deadlock ausgedrückt wird. Analog zu den Pfaden in Berechnungsbäumen lassen sich Folgen von Aktionen - die wir Abläufe (traces) nennen - betrachten.

So besagt etwa $\langle \alpha_1 \rangle \ldots \langle \alpha_n \rangle\, \mathbf{tt}$, daß (von einem best. Zustand aus) ein Weg ex., dessen Kanten mit $\alpha_1, \ldots, \alpha_n$ beschriftet sind, in dieser Reihenfolge. Abläufe sind also Wörter über dem Alphabet $\mathcal{A}$ des Transitionssystems, das mithin auch als Automat aufgefaßt werden kann, der die Sprache aller von einem Anfangszustand aus möglichen traces erkennt.

Die Modalitäten „wirken" wie die CTL-Operatoren AX und EX, nur beziehen sie sich auf Kanten anstatt auf Knoten[12], was durch ein letztes Beispiel illustriert sei:

$$[a]\, (\langle - \rangle\, \mathbf{tt} \, \wedge [b, c]\, \mathbf{ff} \,)$$

bedeutet: alle mit a erreichbaren Zustände ($[a]$) haben mind. einen Nachfolger ($\langle - \rangle \mathbf{tt}$) und keiner dieser Nachfolger ist über b oder c erreichbar ($[b, c]\, \mathbf{ff}$). Wie man sieht, kommt man ganz gut ohne Negation aus. Tatsächlich könnte man sie ebensogut auch zulassen - nur brächte dies keinen nennenswerten Vorteil (außer vielleicht, daß dann $[K]$ durch $\neg \langle K \rangle \neg$ definierbar wäre). So jedenfalls ist die Negation sozusagen komplett in die Übergangsrelationen δ_α „verbannt", und etwas ähnliches werden wir für die Zustandsmarkierungen konstruieren, wenn wir jetzt die HM-Logik zum modalen μ-Kalkül μM erweitern. Auf den Grund wird ein weiteres Mal vertröstet.

2.2.2 Modaler μ-Kalkül

μM-Syntax
Wie vorher sei K eine Menge von Aktionen. Die Menge der wohlgeformten μM-Formeln ist eine Obermenge der wohlgeformten HM-Formeln[13]; erweitert um aussagenlogische *Variablen* Z und die extremalen Fixpunktoperatoren μZ und νZ. Wir geben die Syntax diesmal in kompakterer Form an, nämlich als EBNF-Ausdruck[14], wobei Φ hier für *eine*

[12] genaugenommen natürlich auf deren jeweilige Beschriftungen

[13] abgesehen davon, daß wir $\mathbf{tt}$ und $\mathbf{ff}$ in μM als Abkürzungen betrachten, sh. unten

[14] Die Angabe in Erweiterter Backus-Naur-Form ist etwas salopp, da die Menge und ihre Elemente durcheinandergewürfelt werden; es sollte aber klar sein, daß sie einer induktiven Definition entspricht. Ebenfalls salopp ist es, den Punkt am Ende des Ausdrucks wegzulassen, den die EBNF eigentlich verlangt. Auch müßte es eigentlich jeweils Φ anstatt sowohl Φ_1 als auch Φ_2 heißen. In diesem Fall bedeutet „salopp" jedoch (hoffentlich): besser verständlich.

Formel steht und nicht für die Menge aller Formeln (wie vorher immer):

$$\boxed{\Phi \quad ::= \quad Z \;\mid\; \Phi_1 \wedge \Phi_2 \;\mid\; \Phi_1 \vee \Phi_2 \;\mid\; \langle K \rangle\, \Phi \;\mid\; [K]\, \Phi \;\mid\; \mu Z.\Phi \;\mid\; \nu Z.\Phi}$$

tt und **ff** sind definiert als $\nu Z.Z$ bzw. $\mu Z.Z$; Im folgenden steht σ für ein Element aus $\{\mu, \nu\}$. Eine Fixpunktformel hat die Form $\sigma Z.\Phi$, wobei *freie* Vorkommen von Z in Φ durch σZ *gebunden* werden. Ein Vorkommen von Z ist frei, wenn es sich nicht im Geltungsbereich (scope) eines Fixpunktoperators befindet; ganz wie bei $\forall$ und $\exists$. Ebenso binden (in einem anderen Sinne als eben) die unären Operatoren $\langle\ \rangle$ und $[\ ]$ stärker als $\wedge$ und $\vee$ und diese wiederum stärker als die Fixpunktoperatoren, deren Geltungsbereich somit am größten ist[15].

μM-Semantik

Da wir nun mit möglichen freien Variablen in (Sub-)Formeln umgehen müssen, definieren wir die Modellbeziehung (Erfüllungsrelation) $\models$ indirekt über die Menge derjenigen Zustände, in denen Φ gilt; dies hatten wir im Abschnitt über CTL als Erfüllungsmenge bezeichnet. Dabei verwenden wir eine *Belegung* $\mathcal{V}$(Valuation), die jeder Variablen Z eine Menge $\mathcal{V}(Z)$ von Zuständen in S zuordnet (in denen die Variable als mit **tt** belegt gelten soll), *relativ zu der* die Erfüllungsmenge $\|\Phi\|_{\mathcal{V}}^{S} \subseteq S$ definiert wird und wobei das Superskript S auch gleich wieder fallengelassen wird, wenn die Zustandsmenge klar ist. Eine Belegung funktioniert also genau andersherum wie die bisherige Labellingfunktion l. Man kann nun die Propositionen $p \in P$ im Bild von l ebenfalls als Variablen betrachten und zu jedem p eine weitere neue Variable $\overline{p}$, die Komplementvariable zu p einführen. Sei $\overline{P}$ die Menge der neuen Komplementvariablen. Wenn man annimmt, daß f.a. (betrachteten) $\mathcal{V}$ gilt:

$$\forall p \in P, s \in S : s \in \mathcal{V}(p) \Leftrightarrow p \in l(s)$$
$$\forall \overline{p} \in \overline{P}, s \in S : s \in \mathcal{V}(\overline{p}) \Leftrightarrow p \notin l(s)$$

dann sind die Zustandsmarkierungen in die Belegung kodiert.

Um die Semantik der Modalitäten $[\ ]$ und $\langle\ \rangle$ angeben zu können, brauchen wir Funktionen $\delta^{-1}_{\langle K \rangle}$ und $\delta^{-1}_{[K]}$ analog zu $\delta^{-1}_{\exists}$ bzw. $\delta^{-1}_{\forall}$ aus dem Abschnitt über CTL. Zu jedem $K \subseteq \mathcal{A}$ seien also:

$$\begin{aligned} \delta^{-1}_{\langle K \rangle} :\ & 2^S \to 2^S \\ T \mapsto\ & \{\, s \in S \mid \exists \alpha \in K,\, t \in T : (s,t) \in \delta_\alpha \,\} \end{aligned}$$

$$\begin{aligned} \delta^{-1}_{[K]} :\ & 2^S \to 2^S \\ T \mapsto\ & \{\, s \in S \mid \forall \alpha \in K,\, t \in S : (s,t) \in \delta_\alpha \Rightarrow t \in T \,\} \end{aligned}$$

$\delta^{-1}_{\langle K \rangle}(T)$ ist die Menge von Vorgängern von Zuständen in T, von denen aus man über *eine* α-Kante, $\alpha \in K$ zu einem Zustand in T kommt. Umgekehrt gilt also für jeden dieser Vorgängerzustände: *es gibt* einen α-Nachfolger $t \in T$. Dies benötigen wir für

[15] der Leser möge dieses schöne Beispiel seiner Sammlung an zirkulären Definitionen einverleiben

$\|\langle K\rangle\|$.
$\delta^{-1}_{[K]}(\,T\,)$ ist die Menge von Vorgängern von Zuständen in T, von denen aus man über α-Kanten, $\alpha \in K$ *ausschließlich* zu Zuständen in T kommt[16]. Umgekehrt gilt also für jeden dieser Vorgängerzustände: *alle* α-Nachfolger liegen in T. Dies benötigen wir für $\|[K]\,\|$.
Analog zu dort gilt auch hier:

$$\begin{aligned}\delta^{-1}_{\langle K\rangle}(\,T\,) &= \{\,s \in S \mid \exists\alpha \in K : \delta_\alpha(s) \cap T \neq \emptyset\,\}\\ \delta^{-1}_{[K]}(\,T\,) &= \{\,s \in S \mid \forall\alpha \in K : \delta_\alpha(s) \subseteq T\,\}\end{aligned}$$

bzw.

$$\begin{aligned}\delta^{-1}_{\langle K\rangle}(\,T\,) &= \{\,s \in S \mid (\bigcup_{\alpha\in K} \delta_\alpha(s)) \cap T \neq \emptyset\,\}\\ \delta^{-1}_{[K]}(\,T\,) &= \{\,s \in S \mid (\bigcup_{\alpha\in K} \delta_\alpha(s)) \subseteq T\,\}\end{aligned}$$

Offensichtlich ist $\delta^{-1}_{\langle -\rangle}(\,T\,) = \delta^{-1}_{\exists}(\,T\,)$ und $\delta^{-1}_{[-]}(\,T\,) = \delta^{-1}_{\forall}(\,T\,)$ (dh. falls $K = \mathcal{A}$; sh. 1.3).

Eine Notation für Ersetzung in einer Belegung komplettiert die technischen Hilfsmittel: mit $\mathcal{V}[T/Z]$ wird diejenige Belegung $\mathcal{V}'$ bezeichnet, die mit $\mathcal{V}$ in jedem Punkt übereinstimmt bis auf Z, wo $\mathcal{V}'(Z) = T$ ist.
Die Semantik einer μM-Formel ist nun induktiv gegeben durch:

$$\begin{aligned}\|Z\|_{\mathcal{V}} &= \mathcal{V}(Z)\\ \|\Phi \wedge \Psi\|_{\mathcal{V}} &= \|\Phi\|_{\mathcal{V}} \cap \|\Psi\|_{\mathcal{V}}\\ \|\Phi \vee \Psi\|_{\mathcal{V}} &= \|\Phi\|_{\mathcal{V}} \cup \|\Psi\|_{\mathcal{V}}\\ \|[K]\,\Phi\|_{\mathcal{V}} &= \delta^{-1}_{[K]}(\,\|\Phi\|_{\mathcal{V}}\,)\\ \|\langle K\rangle\,\Phi\|_{\mathcal{V}} &= \delta^{-1}_{\langle K\rangle}(\,\|\Phi\|_{\mathcal{V}}\,)\\ \|\nu Z.\Phi\|_{\mathcal{V}} &= \bigcup\{\,T \subseteq S \mid T \subseteq \|\Phi\|_{\mathcal{V}[T/Z]}\,\}\\ \|\mu Z.\Phi\|_{\mathcal{V}} &= \bigcap\{\,T \subseteq S \mid \|\Phi\|_{\mathcal{V}[T/Z]} \subseteq T\,\}\end{aligned}$$

Die Menge der Zustände mit der Eigenschaft Z ist vollständig bestimmt durch die Funktion $\mathcal{V}$ (die sich, wie wir vereinbart haben, an die Labellingfunktion l „hält“, was Propositionen anbelangt). Die semantischen Klauseln für $\wedge$ und $\vee$ sind wie bei CTL und auch die Klauseln für die modalen Operatoren sind ganz analog zu dort, nur daß die Sache ein wenig komplizierter geworden ist, weil wir nun zwischen Kanten mit verschiedenen Beschriftungen unterscheiden können. Die abgeleiteten Klauseln für die booleschen Konstanten sind ebenfalls $\|\mathbf{tt}\,\|_{\mathcal{V}} = S$ bzw. $\|\mathbf{ff}\,\|_{\mathcal{V}} = \emptyset$.

Monotonie induzierter Funktionen

Jede Formel Φ mit einer[17] freien Variablen Z induziert eine Funktion $\lambda T.\,\|\Phi\|^S_{\mathcal{V}[T/Z]}$:

[16] Man beachte, daß in der Definition von $\delta^{-1}_{[K]}(\,T\,)$ über alle $t \in S$ quantifiziert wird, nicht etwa nur über die in T!

[17] wir betrachten nur den einstelligen Fall. Formeln ohne freie Variablen induzieren konstante Funktionen, z.B. induziert **ff** die Funktion $\lambda T.\emptyset$. Formeln mit mehreren freien Variablen lassen sich durch Currying auf den einstelligen Fall reduzieren.

$2^S \to 2^S$, dh. eine Fkt., die eine Menge von Zuständen $T \subseteq S$ auf die Erfüllungsmenge von Φ bzgl. der Belegung $\mathcal{V}$ abbildet, wobei $\mathcal{V}(Z) = T$. Jede solche Funktion ist monoton bzgl. $\subseteq$ (o.B.). Dies ist auch der oben angekündigte Grund, warum in μM keine Negation vorgesehen ist, denn z.B. die (hypothetische) Formel $\neg Z$ mit der intendierten Bedeutung $\|\neg Z\|_{\mathcal{V}} = S \setminus \|Z\|_{\mathcal{V}} = S \setminus \mathcal{V}(Z)$ induziert die Funktion $\lambda T.S \setminus T$, die offensichtlich nicht monoton ist[18].

Dennoch ist das Komplement einer jeden Formel ebenfalls in der Logik enthalten. Bezeichne $\overline{\Phi}$ das Komplement von Φ, das induktiv wie folgt definiert wird (für $Z \notin P \cup \overline{P}$; das Komplement $\overline{p} \in \overline{P}$ zu $p \in P$ wurde oben schon definiert):

$$
\begin{array}{lcllcl}
\overline{Z} & = & Z & & & \\
\overline{\mathbf{tt}} & = & \mathbf{ff} & \overline{\mathbf{ff}} & = & \mathbf{tt} \\
\overline{\Phi \wedge \Psi} & = & \overline{\Phi} \vee \overline{\Psi} & \overline{\Phi \vee \Psi} & = & \overline{\Phi} \wedge \overline{\Psi} \\
\overline{[K]\,\Phi} & = & \langle K \rangle\,\overline{\Phi} & \overline{\langle K \rangle\,\Phi} & = & [K]\,\overline{\Phi} \\
\overline{\nu Z.\Phi} & = & \mu Z.\overline{\Phi} & \overline{\mu Z.\Phi} & = & \nu Z.\overline{\Phi}
\end{array}
$$

Es folgt, daß $\overline{\overline{\Phi}} = \Phi$ und $\left\|\overline{\Phi}\right\|^S = S \setminus \|\Phi\|$, unabhängig von $\mathcal{V}$.

Da wir also völlig ohne Negation auskommen und so die Monotonie der durch Formeln induzierten Funktion auf Zustandsmengen garantiert ist, stellt die Semantik der Fixpunktformeln nun einfach eine Anwendung des Theorems von Knaster-Tarski dar:

Der größte Fixpunkt ist die Vereinung aller Postfixpunkte und der kleinste Fixpunkt ist die Schnittmenge aller Präfixpunkte.

Eine Konsequenz daraus (Stichwort Approximanden) ist, daß die Bedeutung von $\sigma Z.\Phi$ dieselbe ist wie die der Auffaltung (unfolding) $\Phi_{[\sigma Z.\Phi/Z]}$. So ist z.B. die Auffaltung von $\nu Z.\Phi \wedge \langle - \rangle\, Z$ gleich $\Phi \wedge \langle - \rangle\, \nu Z.\Phi \wedge \langle - \rangle\, Z$ und beide werden von derselben Menge von Zuständen erfüllt. Dies ist uns bei den Erfüllungsmengen für CTL-Formeln schon begegnet und so ist es nun auch nicht mehr schwer, eine Übersetzung von CTL nach μM anzugeben.

[18] Es ist nicht notwendig, $\neg$ komplett zu verbieten, denn nicht alle Formeln, die es enthalten induzieren nicht-monotone Funktionen. Es genügt zu verlangen, daß durch einen Fixpunktoperator gebundene Variablen unter einer *geraden* Anzahl von Negationszeichen erscheinen.

2.2.3 Einbettung von CTL in μM

CTL	Auffaltung	CTL-Erf.-menge	μM
p		$\{ s \in S \mid p \in l(s) \}$	p
$\neg\varphi$		$S \setminus \lVert\varphi\rVert$	$\overline{\varphi}$
$\varphi \wedge \psi$		$\lVert\varphi\rVert \cap \lVert\psi\rVert$	$\varphi \wedge \psi$
$\varphi \vee \psi$		$\lVert\varphi\rVert \cup \lVert\psi\rVert$	$\varphi \vee \psi$
EX φ		$\delta_\exists^{-1}(\lVert\varphi\rVert)$	$\langle - \rangle\, \varphi$
AX φ		$\delta_\forall^{-1}(\lVert\varphi\rVert)$	$[-]\, \varphi$
EF φ	$\varphi\ \vee$ EX EF φ	$\mu T. \lVert\varphi\rVert \cup \delta_\exists^{-1}(T)$	$\mu Z. \varphi\ \vee \langle - \rangle\, Z$
AG φ	$\varphi\ \wedge$ AX AG φ	$\nu T. \lVert\varphi\rVert \cap \delta_\forall^{-1}(T)$	$\nu Z. \varphi\ \wedge [-]\, Z$
EG φ	$\varphi\ \wedge$ EX EG φ	$\nu T. \lVert\varphi\rVert \cap \delta_\exists^{-1}(T)$	$\nu Z. \varphi\ \wedge \langle - \rangle\, Z$
AF φ	$\varphi\ \vee$ AX AF φ	$\mu T. \lVert\varphi\rVert \cup \delta_\forall^{-1}(T)$	$\mu Z. \varphi \vee [-]\, Z$
φ EU ψ	$\psi \vee (\varphi \wedge$ EX EU $\psi)$	$\mu T. \lVert\psi\rVert \cup (\lVert\varphi\rVert \cap \delta_\exists^{-1}(T))$	$\mu Z. \psi \vee (\varphi\ \wedge \langle - \rangle\, Z)$
φ AW ψ	$\psi \vee (\varphi \wedge$ AX AW $\psi)$	$\nu T. \lVert\psi\rVert \cup (\lVert\varphi\rVert \cap \delta_\forall^{-1}(T))$	$\nu Z. \psi \vee (\varphi\ \wedge [-]\, Z)$
φ AU ψ	$\psi \vee (\varphi \wedge$ AX AU $\psi)$	$\mu T. \lVert\psi\rVert \cup (\lVert\varphi\rVert \cap \delta_\forall^{-1}(T))$	$\mu Z. \psi \vee (\varphi\ \wedge [-]\, Z)$
φ EW ψ	$\psi \vee (\varphi \wedge$ EX EW $\psi)$	$\nu T. \lVert\psi\rVert \cup (\lVert\varphi\rVert \cap \delta_\exists^{-1}(T))$	$\nu Z. \psi \vee (\varphi\ \wedge \langle - \rangle\, Z)$

3 Spiele: ∀belard vs. ∃loise

μM-Formeln drücken Eigenschaften von Zustandsübergangssystemen aus. Um welche Eigenschaft es sich bei einer gegebenen Formel handelt ist jedoch nicht in jedem Fall sofort offensichtlich, wie z.B. bei der folgenden:

$$\nu X.\, \langle b \rangle\, \mu Y.\, \langle a \rangle\, X \vee \langle b \rangle\, Y$$

Hier alternieren die beiden Fixpunktoperatoren und die Variable des äußeren tritt im Körper der inneren Fixpunktformel wieder auf. Man kann also nicht die innere Formel ein (und für alle Mal) auswerten, dh. die Erfüllungsmenge bestimmen, denn diese hängt auch vom äußeren Fixpunktoperator ab.
Ein weiteres Beispiel ist

$$\mu X.[-]\, X$$

- kürzer, aber nicht unbedingt klarer.

Um es vorwegzunehmen: die erste Formel besagt, daß es einen Pfad gibt, der mit einem b beginnt und auf dem sowohl a als auch b unendlich oft vorkommen, jedoch niemals zwei a aufeinanderfolgen. Die möglichen traces auf einem solchen Pfad sind die Wörter $(bb^*a)^\omega$.
Die zweite Formel gilt in *endlichen* Systemen ohne Schleifen in jedem Zustand, in einem *unendlichen* System hingegen oder falls Schleifen existieren kann sie von allen, einigen oder überhaupt keinen Zuständen erfüllt sein: sie drückt aus, daß alle Pfade endlich sind.

Die Modelchecking-Spiele, die wir nun betrachten, helfen zu verstehen, welche Eigenschaften durch Formeln charakterisiert werden. Außerdem läßt sich aus ihnen auch ein Modelchecking-Algorithmus ableiten.

3.1 Spielregeln und Gewinnkonditionen

Gegeben sind ein Transitionssystem, ein Zustand daraus sowie eine Formel. Es treten zwei Spieler gegeneinander an. Der eine, im folgenden der universelle Spieler oder ∀belard genannt, versucht die Formel zu *widerlegen*. Seine Gegnerin, die existentielle Spielerin oder ∃loise versucht hingegen die Formel zu beweisen.
Eine *Partie* ist eine Folge von *Konfigurationen* s, φ, die aus einem Zustand s und einer (Teil-)Formel φ bestehen. Ein *Zug* eines Spielers ist die Wahl eines Nachfolgezustandes von s bzw. einer Teilformel von φ. Ein Spiel $\mathcal{G}(s, \varphi)$ mit der Anfangskonfiguration s, φ kann demnach als Baum aufgefaßt werden, dessen Äste Partien sind.
Welcher Spieler am Zug ist und welche Wahl er/sie treffen darf bzw. wann eine Partie endet, wird durch die folgenden Regeln festgelegt:

$$\frac{s, \varphi \vee \psi}{s, \varphi \quad s, \psi}\ \exists \qquad\qquad \frac{s, \varphi \wedge \psi}{s, \varphi \quad s, \psi}\ \forall$$

$$\frac{s, \langle K \rangle\, \varphi}{t, \varphi}\ \exists, s \overset{\alpha \in K}{\longrightarrow} t \qquad\qquad \frac{s, [K]\, \varphi}{t, \varphi}\ \forall, s \overset{\alpha \in K}{\longrightarrow} t$$

$$\frac{s, \sigma X.\varphi}{s, \varphi_{[U/X]}}\ U \text{ neue Var.} \qquad\qquad \frac{s, U}{\sigma X.\varphi}\ \text{vorher: } [U/X] \text{ bei } \sigma X.\varphi$$

$\forall$belard gewinnt, wenn

$\forall$1) s, p und $p \notin l(s)$

$\forall$2) $s, \langle K \rangle \varphi$ und es ex. kein $\alpha \in K, t \in S : s \xrightarrow{\alpha} t$

$\forall$3) (mind.) eine durch einen Fixpunktoperator gebundene Variable unendlich oft ersetzt würde und die äußerste solche Variable durch ein μ gebunden ist.

$\exists$loise gewinnt, wenn

$\exists$1) s, p und $p \in l(s)$

$\exists$2) $s, [K] \varphi$ und es ex. kein $\alpha \in K, t \in S : s \xrightarrow{\alpha} t$

$\exists$3) (mind.) eine durch einen Fixpunktoperator gebundene Variable unendlich oft ersetzt würde und die äußerste solche Variable durch ein ν gebunden ist.

Es muß also $\exists$loise eine Disjunktion durch die Wahl eines wahren Disjunktionsgliedes beweisen, $\forall$belard muß die Falschheit einer Konjunktion durch die Wahl eines falschen Konjunktionsgliedes zeigen. Ist das nicht möglich, weil beide Disjunktionsglieder falsch bzw. beide Konjunktionsglieder wahr sind, gewinnt der jeweils andere.
Eine Existenzaussage $\langle K \rangle \varphi$ über Nachfolgezustände *be*legt $\exists$loise durch die Wahl eines entsprechenden Nachfolgers, desgleichen *wider*legt $\forall$belard eine Allaussage $[K] \varphi$ über Nachfolgezustände. Wieder gewinnt der jeweils andere, wenn das nicht möglich ist weil keine Nachfolgezustände existieren.
Auch die dritten Gewinnkonditionen sind zueinander dual. Sie lassen sich informell etwa so umschreiben: Ist ein Spieler gezwungen - da er/sie ansonsten nach Kondition 1) oder 2) verlieren würde - sich sozusagen immer wieder in eine Fixpunktabwicklung zu flüchten (und so die Widerlegung bzw. den Beweis auf ewig schuldig zu bleiben), so gilt dies als Spielverderberei und wird mit dem Verlust der Partie bestraft. Damit und weil ansonsten die Formeln immer weiter in Subformeln zerlegt werden, ist offensichtlich die Endlichkeit jeder Partie und damit eines jeden Spiels sichergestellt. $\exists$loise muß zeigen, daß kleinste Fixpunkte nicht leer sind, $\forall$belard muß zeigen, daß größte Fixpunkte nicht die gesamte Zustandsmenge umfassen.
$\forall : \|\nu Z.\Phi\| \neq S$
$\exists : \|\mu Z.\Phi\| \neq \emptyset$

3.2 Beweisskizze: $M, s \models \Phi \Leftrightarrow$ es ex. eine Gewinnstrategie für $\exists$loise

Bislang haben wir lediglich erklärt, wann ein Spieler eine *Partie* gewinnt. Natürlich ist auch denkbar, daß ein Spieler eine Partie „unnötigerweise“ verliert, etwa wenn $\forall$belard ungeschickterweise ein wahres Konjunktionsglied wählt bzw. $\exists$loise ein falsches Disjunktionsglied. Der Gewinn eines *Spiels* wird daher definiert über die Möglichkeit, den Sieg in einer Partie zu erzwingen. Wir werden zeigen, daß $\exists$loise im Spiel $\mathcal{G}(s, \varphi)$ genau dann eine für sie siegreiche Partie erzwingen kann, wenn $s \models \varphi$.

Def.: Approximanden:

$$\begin{aligned}\mu^0 X.\psi &:= \mathbf{ff}\\ \mu^{\alpha+1} X.\psi &:= \psi[\mu^\alpha X.\psi/X]\\ \mu^\lambda &:= \bigvee_{\alpha<\lambda} \mu^\alpha X.\psi\end{aligned}$$

Lemma 1: $\exists$ gewinnt $\mathcal{G}(s,\varphi) \Leftrightarrow \forall$ gewinnt $\mathcal{G}(s,\overline{\varphi})$
folgt aus der Endlichkeit jeder Partie und der Dualität von Regeln und Gewinnkonditionen

Lemma 2: $\mathcal{G}(s,\varphi)$ ist determiniert.
Regeln und Gewinnkonditionen sind erschöpfend. Beachte: Im Falle unendlicher Systeme kann es unendlich viele Nachfolger zu einem oder mehreren Zuständen geben. Der Baum $\mathcal{G}s,\varphi$ hat dann zwar noch endliche Höhe ist aber (stellenweise) unendlich verzweigt.

Lemma 3: Wenn $s \models \varphi$, dann kann $\exists$die Wahrheit in allen Nachfolgekonfigurationen s',φ' erhalten.
In den Regeln 3 findet eine rein syntaktische Ersetzung statt, was an der Modellbeziehung nichts ändert. Ist $\exists$ nach Regel 1 oder 2 am Zug, so ergibt sich die Möglichkeit direkt aus der Semantik. Ist hingegen $\forall$ am Zug, so gilt nach der Semantik von $\wedge$ bzw. $[K]$ bei *jeder* seiner Wahl die Modellbeziehung weiter.

Lemma 4: $s \models \mu X.\varphi \Leftrightarrow \exists\alpha \in \mathrm{Ord} : s \models \mu^\alpha X.\varphi$

Theorem: $\exists$ hat Gewinnstrategie für $\mathcal{G}(s,\varphi) \Leftrightarrow s \models \varphi$

Beweis:
„$\Rightarrow$“: Angenommen $\exists$ gewinnt $\mathcal{G}(s,\varphi)$. Dann nach Lemma 1: $\forall$ gewinnt $\mathcal{G}(s,\overline{\varphi})$. Außerdem: $\forall$ gewinnt $\mathcal{G}(t,\overline{\psi}) \implies t \not\models \psi$ (Kontraposition von „$\Leftarrow$“ und Lemma 2) Also $s \not\models \overline{\varphi}$ bzw. $s \models \varphi$

„$\Leftarrow$“: Angenommen $s \models \varphi$. Die Strategie σ „erhalte Wahrheit“ ist eine Gewinnstrategie, dh. jede Partie π, in der $\exists$nach σ spielt (und $\forall$nach beliebiger) wird von $\exists$gewonnen. Angenommen $\forall$gewinnt π. Gewinnbedingungen $\forall$1) und $\forall$2) widersprechen sofort σ und Lemma 3.
Angenommen $\forall$gewinnt nach $\forall$3). Dh.:

$$\pi = (s,\varphi),\ldots,(t_0,\mu Y.\psi),(t_0,Y),(t_0,\psi),\ldots,(t_1,Y),\ldots,(t_2,Y),\ldots$$

Y ist die äußerste Variable, gebunden durch μ. Nach σ sind alle Konfigurationen in π wahr, insbesondere (t_0,Y), also $t_0 \models \mu Y.\psi$. Nach Lemma 4 existiert ein kleinstes $\alpha \in$ Ord, sd. $t_0 \models \mu^\alpha Y.\psi$. Interpretiere (t_0,Y) als $(t_0,\mu^\alpha Y.\psi)$:

$$\pi = (s,\varphi),\ldots,(t_0,\mu Y.\psi),(\overset{\alpha}{t_0},Y),(t_0,\psi),\ldots,(\overset{\alpha-1}{t_1},Y),\ldots,(\overset{\cdots}{t_2},Y),\ldots$$

(t_i,Y) zeigt $t_i \models \mu^{\alpha-i}Y.\psi$. Falls $\alpha - i$ ein Limitordinal ist, dann ex. $\beta < \alpha - i$, sd. $t_i \models \mu^\beta Y.\psi$. Ordinale sind wohlfundiert, also ex. $k \in \mathbb{N}$, sd. (t_k,Y) ein Beweis ist für $t_k \models \mu^0 Y.\psi$. Widerspruch.

Also gewinnt $\exists$ jedes solche π und deshalb ist σ Gewinnstrategie.

3.3 Bedeutung von Formeln aus Spielesicht

Betrachten wir zunächst das zweite Beispiel vom Anfang des Abschnitts: $\mu X.[-]\, X$. Hier hat $\exists$loise niemals die Möglichkeit einen Zug zu machen. Ihre einzige Gewinnmöglichkeit ist über $\exists$3). Das Transitionssystem muß also so beschaffen sein, daß unabhängig von $\forall$belard s Wahl irgendwann einmal kein Nachfolger mehr existiert. Das ist genau dann der Fall, wenn (vom Startzustand aus) alle Pfade endlich sind.

Bei $\nu X.\, \langle b\rangle\, \mu Y.\, \langle a\rangle\, X \vee \langle b\rangle\, Y$ hingegen hat $\forall$belard keinerlei Wahlmöglichkeit und kann über $\forall$2) oder $\forall$3) gewinnen.

- Gewinnt er nach $\forall$2), so existierte irgendwann kein b- oder a-Nachfolger mehr, dh. der Pfad enthielt nur endlich viele aufeinanderfolgende a und b.

- Gewinnt er nach $\forall$3), dann wäre Y unendlich oft ersetzt worden, aber nicht X, dh. $\exists$loise war gezwungen, immer wieder nur das zweite Disjunktionsglied $\langle b\rangle\, Y$ zu wählen. Es waren also irgendwann nur noch b- aber keine a-Nachfolger erreichbar, mithin kann es vorher nur endlich viele a gegeben haben.

- Falls jedoch $\exists$loise gewinnt, dann nur über $\exists$3) mit X als der unendlich oft ersetzten Variable. Nach jeder Ersetzung von X durch U_i muß aber die Teilformel $\langle b\rangle\, \mu Y.\, \langle a\rangle\, U_i \vee \langle b\rangle\, Y$ abgebaut werden, mithin ein b vorkommen, insbes. am Anfang der Partie. Danach folgt eine Ersetzung von Y durch W_j und die Formel $\langle a\rangle\, U_i \vee \langle b\rangle\, W_j$ wird untersucht. Bei der späteren (nach mind. einem a und beliebig aber endlich vielen b, also $i \leq j$) Ersetzung von U_i durch die Ausgangsformel $\nu X.\, \langle b\rangle\, \mu Y.\, \langle a\rangle\, X \vee \langle b\rangle\, Y$ steht wieder ein b an. Deshalb können keine zwei a aufeinanderfolgen.

4 Anhang: Verbände und Fixpunkte

(Mitschrift des Vortrags von M. Lange am 10.11.2004)

4.1 Verbände

Sei M eine Menge und $\leq \subseteq M \times M$.
$\leq$ heißt partielle Ordnung falls

- $\forall x \in M : x \leq x$ (Reflexivität)
- $\forall x, y \in M : x \leq y$ und $y \leq x \Rightarrow x = y$ (Antisymmetrie)
- $\forall x, y, z \in M : x \leq y$ und $y \leq z \Rightarrow x \leq z$ (Transitivität)

Sei $N \subseteq M$, dann heißt y *obere Schranke* von N, falls
$\forall x \in N : x \leq y$

y heißt *Supremum* (kleinste obere Schranke), falls
y obere Schranke für N ist und f.a. oberen Schranken z für N: $y \leq z$

x heißt *untere Schranke* von N, falls
$\forall y \in N : x \leq y$

x heißt *Infimum* (größte untere Schranke), falls
x untere Schranke für N ist und f.a. unteren Schranken z für N: $x \geq z$

Notation: falls $N = \{x, y\}$, dann schreiben wir $x \sqcup y$ für das Supremum von N und $x \sqcap y$ für das Infimum von N und sonst

für $N \subseteq M$:
$\bigsqcup N := \{\, x \in M \mid \forall y \in N : x \sqcup y = x \,\}$
$\bigsqcap N := \{\, x \in M \mid \forall y \in N : x \sqcap y = x \,\}$

Ein *Verband* ist ein Paar $(M, \leq)$, so daß
$\forall x, y \in M : x \sqcup y, x \sqcap y \in M$

Bsp.:

a) (k)ein Verband[19]
b) M Menge, $(2^M, \subseteq)$: Verband wobei für $X, Y \in 2^M$:
$X \sqcup Y = X \cup Y$
$X \sqcap Y = X \cap Y$

Ein Verband heißt *vollständig*, falls
$\forall X \subseteq M : \bigsqcup X, \bigsqcap X \in M$

Ein Verband $(M, \leq)$ heißt *boolesch*[20], falls:

1) $\forall x, y, z \in M : x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$ (Distributivität)
2) $\exists \bot, \top \in M, \forall x \in M : \bot \leq x \leq \top$ (Beschränktheit)
3) $\forall x \in M, \exists y \in M : x \sqcup y = \top, x \sqcap y = \bot$ (Existenz d. Komplements)

Bsp. a) von oben ist *kein* boolescher Verband (wg. 3))

Ein boolescher Verband $(M, \leq)$ heißt *distributiv*, falls
$\forall X, Y, Z \in 2^M : X \sqcap (Y \sqcup Z) = (X \sqcap Y) \sqcup (X \sqcap Z)$
wobei $X \sqcap Y := \bigsqcap \{\, x \sqcap y \mid x \in X, y \in Y \,\}$, $X \sqcup Y$ analog.

Bsp.:

[19] haha, hier fehlt das Bild (Hasse-Diagramm)
[20] nicht: kölsch

- nicht vollständiger Verband: $(\mathbb{N}, \leq)$
  denn $\bigsqcap \emptyset$ existiert nicht (und $\bigsqcup \mathbb{N} \notin \mathbb{N}$)
- nicht vollständiger Verband: $(2^{\mathbb{N}}_{fin} = \{\, N \subseteq \mathbb{N} \mid N \text{endlich} \,\}, \subseteq)$
  denn $\bigsqcup \{\, N \subseteq \mathbb{N}_{fin} \mid \forall x \in M : x \text{ gerade} \,\} = \{\, x \mid x \text{ gerade} \,\} \notin 2^{\mathbb{N}}_{fin}$
  oder auch wg. $\bigsqcup 2^{\mathbb{N}}_{fin} = \mathbb{N} \notin 2^{\mathbb{N}}_{fin}$
- ein boolescher Verband, der nicht vollständig ist:
  $(\{\, N \subseteq \mathbb{N} \mid N \text{ endlich oder co-endlich} \,\}, \subseteq)$[21]
  $\rightsquigarrow$ Gegenbeispiel: gerade Zahlen
- $(\mathbb{N}, |)$, wobei $a|b \Leftrightarrow \exists c : c \cdot b = a$ ist ein Verband
  kgV und ggT sind Suprema bzw. Infima, $\perp = 1, \top = 0$

4.2 Fixpunkte

Def.: Sei $(M, \leq)$ ein Verband, $f : M \to M$. Ein $x \in M$ heißt

$$\begin{aligned} \textit{Fixpunkt} \text{ von } f \text{ falls } f(x) &= x \\ \textit{Präfixpunkt} \text{ von } f \text{ falls } f(x) &\leq x \\ \textit{Postfixpunkt} \text{ von } f \text{ falls } x &\leq f(x) \end{aligned}$$

Notation:

$$\begin{aligned} \mu x.f(x) &\ \hat{=}\ \text{kleinster (bzgl. } \leq \text{) Fixpunkt von } \lambda x.f(x) \text{ (falls er ex.)} \\ \nu x.f(x) &\ \hat{=}\ \text{größter (bzgl. } \leq \text{) Fixpunkt von } \lambda x.f(x) \text{ (falls er ex.)} \end{aligned}$$

Bsp.: $M = \{0, 1, 2\}$ $\quad f : 2^M \to 2^M, N \mapsto (N \cap 1,) \cup (\overline{N} \cap 1)$
Post-FP von f : $\emptyset, \{1\}, \{2\}, \{1, 2\}$
Prä-FP von f : $\emptyset, \{1\}, \{1, 2\}, \{0, 1\}, \{0, 1, 2\}$
$\Rightarrow f$ hat 2 FP:
$\mu N.f(N) = \{1\}$
$\nu N.f(N) = \{1, 2\}$

Def.: Sei $(M, \leq)$ ein Verband, $f : M \to M$. f heißt *monoton*, falls
$\forall x, y \in M : x \leq y \Rightarrow f(x) \leq f(y)$

Lemma: $f, g : M \to M$ monoton $\Rightarrow f \circ g$ monoton, denn
$\forall x, y \in M : x \leq y \Rightarrow g(x) \leq g(y) \Rightarrow f(g(x)) \leq f(g(y))$

Theorem (Knaster-Tarski)
Sei $(M, \leq)$ vollständiger Verband, $f : M \to M$ monoton. Dann

$$\begin{aligned} \mu x.f(x) &= \bigsqcap \{\, x \in M \mid f(x) \leq x \,\} \\ \nu x.f(x) &= \bigsqcup \{\, x \in M \mid x \leq f(x) \,\} \end{aligned}$$

Beweis: Sei $P := \{\, x \in M \mid f(x) \leq x \,\}$ und $\alpha := \bigsqcap P$.
Für alle $x \in P : \alpha \leq x$. Aus Monotonie folgt:
$f(\alpha) \leq f(x) \leq x$. Also $f(\alpha) \leq \alpha$ also $\alpha \in P$
Nochmal Monotonie: $f(f(\alpha)) \leq f(\alpha)$. Also $f(\alpha) \in P$. Wg. $\alpha = \bigsqcap P$ (dh. $\forall x \in P : \alpha \leq x$) folgt $\alpha \leq f(\alpha)$, also ist α FP von f.
α ist *kleinster* FP:
Sei β FP von f, also $f(\beta) \leq \beta$ (und damit $\beta \in P$). Also $\alpha \leq \beta$.
$\nu x.f(x)$ analog.

$\square$

[21] eine Menge heißt co-endlich, wenn ihr Komplement endlich ist

Def.: Sei $(M,\leq)$ ein Verband. Die *Höhe* von $(M,\leq)$ ist die Länge einer maximalen Kette $x \leq \ldots \leq y$ verschiedener Elemente.
Beachte: Höhe nicht immer endlich, z.B. $(2^{\mathbb{N}},\subseteq)$

Sei $(M,\leq)$ vollständiger Verband endlicher Höhe, $f : M \to M$ monoton. Dann sind die (k-ten) *Approximanden* des kleinsten und größten Fixpunkts induktiv definiert durch:

$$\begin{array}{ll} \mu^0 x.f(x) = \bot & \mu^{k+1}x.f(x) = f(\mu^k x.f(x)) \\ \nu^0 x.f(x) = \top & \nu^{k+1}x.f(x) = f(\nu^k x.f(x)) \end{array}$$

Lemma: Sei $(M,\leq)$ vollständiger Verband endlicher Höhe $h \in \mathbb{N}$, $f : M \to M$ monoton. Dann gilt:

$$\begin{array}{rcl} \mu x.f(x) & = & \mu^h x.f(x) \\ \nu x.f(x) & = & \nu^h x.f(x) \end{array}$$

Beweis:
„$\geq$“

$\mu^0 x.f(x) = \bot \leq \mu x.f(x)$

$\mu^{k+1}x.f(x) = f(\mu^k x.f(x)) \overset{IV, Monotonie}{\leq} f(\mu x.f(x)) = \mu x.f(x)$

„$\leq$“

Beh.: $f(\mu^h x.f(x)) \leq \mu^h x.f(x)$
$\forall k : \mu^k x.f(x) \leq \mu^{k+1}x.f(x)$ wg. Monotonie
$\bot \leq f(\bot) \leq f(f(\bot)) \leq \ldots = \ldots = \ldots$
falls $\exists k$ mit $\mu^k x.f(x) = \mu^{k+1}x.f(x)$
dann $\forall k' \geq k : \mu^k x.f(x) = \mu^{k'} x.f(x)$
also spätestens nach h Schritten

$\square$

5 Literatur

Literatur

[St04] C. Stirling. Modal and Temporal Logics for Processes. (to appear)

[LSt00] M. Lange and C. Stirling. Model Checking Games for Branching Time Logics. *JLC 12*, pp 623-639 (2000)

Dec. 17, 2004: available at `http://homepages/inf.ed.ac.uk/cps/`

[St89] C. Stirling, Comparing Linear and Branching Time Temporal Logics. *LNCS 398*, pages 1-20 (1989)

[Koz82] D. Kozen, Results on the propositional mu-calculus. *LNCS* 140, pp. 333-345 (1982) *TCS* 27, pages 333-354 (1983)

[HM80] Hennessy, M. and Milner, R. On observing nondeterminism and concurrency. *LNCS* 85, pp. 295-309 (1980)

[HM85] Hennessy, M. and Milner, R. Algebraic laws for nondeterminism and concurrency. *Journal of the ACM* 32, pp. 137-162 (1985)