Leibniz Universität Hannover
Fakultät für Elektrotechnik und Informatik
Institut für Theoretische Informatik

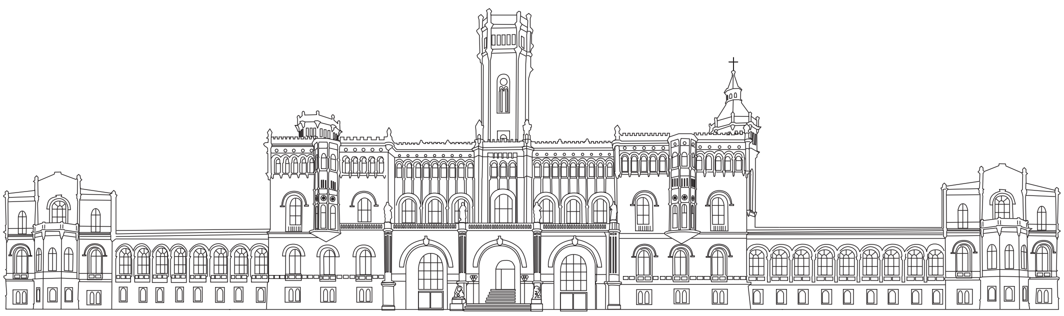
Bachelorarbeit

Endliche Modelleigenschaft in modaler Logik

Finite model property in modal logic

Tobias Brockmeyer
Matrikelnr. 10011858

25. August 2020



Erstprüfer:	Prof. Dr. rer. nat. Heribert Vollmer
Zweitprüfer:	PD Dr. rer. nat. habil. Arne Meier
Betreuer:	M. Sc. Timon Barlag

Hiermit versichere ich, dass ich diese Arbeit selbstständig verfasst habe, keine anderen als die angegebenen Quellen und Hilfsmittel benutzt wurden, alle Stellen der Arbeit, die wörtlich oder sinngemäß aus anderen Quellen übernommen wurden, als solche kenntlich gemacht sind, und die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen hat.

Hannover, 1. Oktober 2020

Tobias Brockmeyer

Inhaltsverzeichnis

1 Einleitung **1**

2 Grundlagen **3**
2.1 Mathematische Grundlagen 3
2.2 Mehrdimensionale Modallogik 4
2.3 Computation Tree Logic 8
2.3.1 CTL 9
2.3.2 LTL 12
2.4 Endliche Modelleigenschaft 13

3 Einfache Modallogik **15**
3.1 Eindimensionale Konnektoren 15
3.1.1 Einfache Modallogik 15
3.1.2 Modallogisches Erfüllbarkeitsproblem 19
3.2 Verallgemeinerungen 20
3.2.1 Multi-Modallogik 20
3.2.2 Rahmeneigenschaften 21
3.3 Mehrdimensionale Konnektoren 24

4 Temporale Logik **31**
4.1 CTL 31
4.2 LTL 40

5 Zusammenfassung **43**

1 Einleitung

Durch die zunehmende Digitalisierung werden heutzutage immer komplexere Probleme durch Software gelöst. Die entstehenden Programme sind in der Regel sehr umfangreich und die Probleme, die durch sie gelöst werden sollen, teilweise sicherheitsrelevant. Wenn Software in medizinischen Geräten in Krankenhäusern beispielsweise versagt, sind die Folgen schwerwiegend.

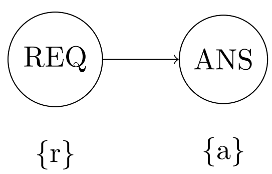
Der Funktionsumfang moderner Software ist zudem meist so umfangreich, dass erschöpfendes Testen aller Features und Eingabemöglichkeiten oftmals unmöglich ist.

Aus diesem Grund ist es sinnvoll, Software formal mathematisch überprüfen zu können. Bestimmte Mindestanforderungen, die die Software im schlimmsten Fall gewährleisten muss, können in einem mathematischen Modell der Software formalisiert und anschließend mit verfügbaren Model Checkern verifiziert oder falsifiziert werden [3, 6].

Eine mathematische Möglichkeit, Aussagen zu formalisieren, ist die Aussagenlogik. In der Aussagenlogik ist es möglich, durch das Einführen entsprechender Variablen Aussagen wie „Das Gerät ist eingeschaltet.“ oder „Auf dem Display steht ‚Willkommen!‘“ auszudrücken. Für eine Mikrowelle kann z.B. durch die Formel

$$\text{Mikrowelle aktiv} \rightarrow \text{Tür ist geschlossen}$$

formalisiert werden, dass die Mikrowelle nur arbeiten soll, wenn die Tür geschlossen ist. Aussagenlogik setzt jedoch voraus, dass alle Variablen zeitinvariant sind, d.h. eine Variable kann wahr oder falsch sein, diesen Zustand aber über die Zeit nicht ändern. Problematisch ist das z.B. bei Systemen, die einem Nutzer eine Antwort generieren sollen, nachdem er eine Anfrage gestartet hat. Die Antwort wird erst erfolgen, *nachdem* die Anfrage erfolgt ist. Gleichzeitig ist die Anfrage eine kurze, abgeschlossene Handlung, d.h. beides erfolgt nicht gleichzeitig. Wenn wir ein solches Verhalten modellieren wollen, sollten wir Aussagen daher nicht zeitunabhängig, sondern zu gewissen Zeitpunkten auswerten. Das können wir mithilfe von Modallogik tun und unsere Anforderung mit $r \rightarrow \Diamond a$ (r modelliert den Request, a die Antwort) formalisieren. Ein entsprechendes Modell wäre:



Auch hier gibt es Grenzen: Möglicherweise soll ein Programm, bevor es eine Antwort ausgibt, erst einige Zwischenschritte als Berechnung durchführen. In diesem Fall interessiert uns nicht, ob die Antwort im nächsten Schritt erfolgt, sondern wir sind vor allem daran interessiert, dass sie überhaupt erfolgt. Auch hierfür gibt es eine Lösung, nämlich die temporale Logik, die im Detail im zweiten Kapitel eingeführt wird.

Solche Anwendungen, aber auch z.B. philosophische Anwendungen motivieren die genauere mathematische Untersuchung der genannten Logik-Varianten. Da es in der Mathematik keine Ressourcengrenzen gibt, haben wir es an vielen Stellen mit Unendlichkeit zu tun. Prinzipiell können wir unendliche Modelle für modal- und temporallogische Formeln konstruieren und Formeln darauf auswerten. In dieser Arbeit soll untersucht werden, ob das nötig ist.

Konkret soll es um die Fragestellung gehen, ob eine erfüllbare aussagenlogische Formel stets bereits auf einem endlichen Modell erfüllt werden kann oder ob es Formeln gibt, die nur auf unendlichen Modellen erfüllt werden können. Die Eigenschaft, dass endliche Modelle zur Erfüllung von Formeln stets ausreichen, nennen wir endliche Modelleigenschaft. Die endliche Modelleigenschaft ist aus mathematischer Sicht z.B. für Entscheidbarkeitsprobleme relevant, wie im dritten Kapitel exemplarisch gezeigt wird.

Im folgenden Kapitel sind zunächst die nötigen Grundlagen und Notationen dargestellt. Dort werden wir unter anderem den Begriff der endlichen Modelleigenschaft formal einführen, die temporale Logik CTL^* mit ihren Spezialfällen LTL (Linear Temporal Logic) und CTL (Computation Tree Logic) definieren und eine mehrdimensionale Variante der Modallogik vorstellen.

Das dritte Kapitel befasst sich mit der einfachen Modallogik und ihren mehrdimensionalen Varianten. Die dort betrachteten Logiken haben alle die Gemeinsamkeit, dass die modallogischen Operatoren, die für sie definiert sind, nur eine Kante weit schauen können. Wir werden für all diese Varianten die endliche Modelleigenschaft nachweisen und am Ende des Kapitels kurz darauf eingehen, welche Auswirkung die Einschränkung verwendeter Rahmen auf dieses Resultat hat.

Schließlich ist das Thema des vierten Kapitels die temporale Logik mit dem Schwerpunkt auf der endlichen Modelleigenschaft der Berechnungsbaumlogik CTL. Am Ende des Kapitels wird außerdem kurz betrachtet, warum LTL die endliche Modelleigenschaft nicht besitzt.

2 Grundlagen

Grundlage für die Betrachtung der endlichen Modelleigenschaft sind die in [1] eingeführte von einer modalen Basis (engl. *modal similarity type*) abhängige Modallogik sowie zwei Varianten der Temporallogik, die sich der Berechnungsbaumlogik (CTL^*) wie sie in [5] definiert wird zuordnen lassen. Für LTL verwenden wir die Definition aus [3] sowie einige Notationen aus [6]. Die nachfolgend eingeführten modallogischen Definitionen entsprechen daher denen aus [1], [5] und [6].

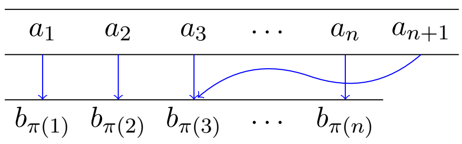
Zudem wird am Ende des Kapitels eingeführt, was es für eine Modallogik heißt, die endliche Modelleigenschaft [1] zu besitzen, um anschließend in den nachfolgenden Kapiteln Techniken zu zeigen, mit denen die endliche Modelleigenschaft gewisser Modallogik-Varianten gezeigt oder widerlegt werden kann.

2.1 Mathematische Grundlagen

In diesem Abschnitt sind zunächst einige grundlegende mathematische Resultate zusammengestellt, die nicht im direkten Zusammenhang zur Modallogik stehen, in den folgenden Betrachtungen allerdings vorausgesetzt werden. Die in dieser Arbeit verwendete Definition der natürlichen Zahlen ist $\mathbb{N} = \{0, 1, 2, \dots\}$ bzw. $\mathbb{N}^* = \{1, 2, \dots\}$.

Lemma 2.1. *Es seien A, B Mengen mit $B = \{b_1, \dots, b_n\}$ und $f\colon A \to B$ eine injektive Funktion. Dann gilt $|A| \leq n$.*

Beweis. Angenommen, es gilt $|A| > n$. Dann seien $a_1, a_2, \dots, a_{n+1} \in A$, sodass $a_i \neq a_j$ für alle $i \neq j$. Es folgt aufgrund der Injektivität von f, dass ein $\pi \in S_n$ existiert, sodass $(f(a_1), f(a_2), \dots, f(a_n)) = (b_{\pi(1)}, b_{\pi(2)}, \dots, b_{\pi(n)})$.



Da aber $f(a_{n+1}) \in B$, also $f(a_{n+1}) = b_i$ für ein $i \in \{1, \dots, n\}$, gilt $f(a_{n+1}) = f(a_{\pi^{-1}(i)})$ und folglich ist f im Widerspruch zur Voraussetzung nicht injektiv. Es folgt also $|A| \leq |B|$. $\square$

Lemma 2.2. *Es sei A eine Menge mit $|A| = n$ und $\mathcal{P}(A) := \{B \mid B \subseteq A\}$ die Potenzmenge von A. Dann gilt $|\mathcal{P}(A)| = 2^n$.*

Beweis. Es sei $A = \{a_1, \dots, a_n\}$. Definiere $f\colon \mathcal{P}(A) \to \{0, 1, \dots, 2^n - 1\}$ durch $X \mapsto \mathsf{VAL}(w_1 w_2 \dots w_n)$, wobei VAL die Abbildung bezeichnet, die ein Binärwort auf ihren Dezimalwert abbildet und

$$w_i = \begin{cases} 1, & a_i \in X \\ 0, & \text{sonst.} \end{cases}$$

f ist bijektiv via $f^{-1}\colon \{0,1,\dots,2^n-1\} \to \mathcal{P}(A)$ mit der Abbildungsvorschrift $n \mapsto \{a_i \mid w_i = 1\}$, wobei $w_1 w_2 \dots w_n$ die (eindeutige) Binärdarstellung von n ist. Damit gilt $|\mathcal{P}(A)| = |\{0,1,\dots,2^n-1\}| = 2^n$. □

Das folgende Lemma ist ein Spezialfall des Unendlichkeitslemmas des ungarischen Mathematikers Denes König, das aussagt, dass in allen unendlichen zusammenhängenden Graphen ein unendlich langer Pfad oder ein Knoten mit unendlich vielen Nachfolgern existiert [7]. Für diese Arbeit benötigen wir nur den Fall, dass der betrachtete Graph ein Baum ist und nehmen an, dass jeder Knoten nur endlich viele Nachfolger hat, um zu zeigen, dass ein unendlicher Pfad existiert.

Lemma 2.3. *Es sei $G = (V, E)$ ein unendlicher gerichteter Baum, wobei alle Knoten in V nur endlich viele Nachfolger haben. Dann gibt es einen unendlich langen einfachen Pfad in G (d.h. einen Pfad, der keinen Knoten mehrmals besucht).*

Beweis. Wir zeigen: Es gibt einen unendlich langen Pfad $v_1, v_2, \dots$ in G, sodass $v_i \neq v_j$ für alle $i \neq j$. Wir zeigen mithilfe von Induktion über i, dass v_i stets einen Nachfolger v_{i+1} mit $v_{i+1} \neq v_j$ für alle $j \neq i+1$ hat, von dem aus unendlich viele Knoten erreichbar sein müssen.

(I.A.) Es sei $v_1 \in V$ die Wurzel von G. Da G unendlich ist, können von v_1 aus unendlich viele Knoten erreicht werden. Zu jedem dieser unendlich vielen Knoten gibt es also einen von v_1 ausgehenden Pfad. Jeder dieser Pfade beginnt mit einem der endlich vielen Nachfolger von v_1. Es muss nun ein $v_2 \in V$ mit $(v_1, v_2) \in E$ geben, sodass von v_2 aus unendlich viele Knoten erreicht werden können.

Anderenfalls können von v_1 aus nur endlich viele Knoten erreicht werden, da v_1 aber die Wurzel ist und alle Knoten aus V von v_1 aus erreicht werden können, ist G dann im Widerspruch zur Annahme endlich.

(I.S.) Da von v_i aus unendlich viele Knoten erreicht werden können, folgt analog wie für den Fall $i = 1$, dass es einen Nachfolger v_{i+1} von v_i geben muss, von dem aus unendlich viele Knoten erreichbar sein müssen. Da G azyklisch ist, ist $v_{i+1} \neq v_j$ für alle $j < i+1$.

□

2.2 Mehrdimensionale Modallogik

Die Untersuchungen in dieser Arbeit behandeln vor allem die aus dem Grundstudium bekannte Modallogik. Zur Abgrenzung wird diese nachfolgend *einfache Modallogik* genannt. Da im dritten Kapitel auch mehrdimensionale modale Konnektoren betrachtet werden, möchte ich zunächst einen flexibleren Begriff der Modallogik einführen, der beliebig viele, insbesondere auch mehrdimensionale Konnektoren erlaubt.

Definition 2.4 (modale Basis – *engl. modal similarity type*)**.** *Eine modale Basis ist ein Tupel $\tau = (O, \rho)$, wobei O eine nichtleere Menge und ρ eine Funktion $O \to \mathbb{N}$ ist. Die Elemente von O werden* modale Konnektoren *genannt und als $\triangle_1, \triangle_2, \dots$ notiert. Die Funktion ρ ordnet jedem modalen Konnektor zu, auf wie viele Argumente er angewandt werden muss. Für $\triangle_i \in O$ mit $\rho(\triangle_i) = 1$ schreiben wir auch $\Diamond_i$.*

Definition 2.5 (Modallogische Formel)**.** *Die Menge der gültigen modallogischen Formeln über einer modalen Basis* $\tau = (O, \rho)$ *nennen wir* FORM_τ*. Es sei* VAR *eine endliche Menge von Variablen.* FORM_τ *enthält genau die folgenden Elemente:*

- *Für alle* $p \in \mathsf{VAR}$ *gilt* $p \in \mathsf{FORM}_\tau$*.*
- *Für* $\phi, \psi \in \mathsf{FORM}_\tau$ *gilt:*
  (1) $\neg\phi \in \mathsf{FORM}_\tau$
  (2) $\phi \wedge \psi \in \mathsf{FORM}_\tau$
- *Für alle* $\triangle \in O$*,* $\phi_1, \ldots, \phi_{\rho(\triangle)} \in \mathsf{FORM}_\tau$ *gilt* $\triangle(\phi_1, \ldots, \phi_{\rho(\triangle)}) \in \mathsf{FORM}_\tau$*.*

Wir führen außerdem die Abkürzungen $\phi \vee \psi := \neg(\neg\phi \wedge \neg\psi)$, $\phi \to \psi := \neg\phi \vee \psi$ und $\phi \leftrightarrow \psi := (\phi \to \psi) \wedge (\psi \to \phi)$ ein.

Die *einfache Modallogik* erhält man nach dieser Definition, indem man die modale Basis $\mathsf{ML} := (\{\Diamond\}, \rho)$ mit $\rho(\Diamond) = 1$ verwendet und $\Box\phi := \neg\Diamond\neg\phi$ für alle $\phi \in \mathsf{FORM}_{\mathsf{ML}}$ setzt. Außerdem sind in Abgrenzung zur Multi-Modallogik nicht nur unäre Konnektoren erlaubt – wir werden in Beispiel 2.8 sehen, wie mehrdimensionale Konnektoren aussehen können. Mit der Einschränkung $\rho(\triangle) = 1$ für alle Konnektoren $\triangle$ einer modalen Basis erhalten wir genau die Multi-Modallogik.

Durch die allgemeinere Fassung der Modallogik ist auch eine Anpassung des Begriffs des Rahmens notwendig. Vergleichbar mit der Multi-Modallogik führen wir hier für jeden modalen Konnektor aus der modalen Basis eine eigene Relation ein. Für den unären Fall entspricht das weiterhin einer Kantenrelation auf den Welten. In allen anderen Fällen weisen wir den Welten Tupel von Nachfolgerwelten zu.

Definition 2.6 (Rahmen, Modell)**.** *Es seien* $\tau = (O, \rho)$ *eine modale Basis und* VAR *eine nichtleere Menge von Variablen.*
Ein τ*-Rahmen ist ein Tupel* $\mathcal{F} = (W, \{R_{\triangle_i} \mid \triangle_i \in O\})$*, wobei*

- W *ist die nichtleere Menge der Welten von* $\mathcal{F}$*,*
- $R_{\triangle_i}$ *ist eine* $(n+1)$*–stellige Relation auf* W*, wobei* $n = \rho(\triangle_i)$*.*

Ein τ*-Modell ist ein Tupel* $\mathcal{M} = (\mathcal{F}, V)$*, wobei* $\mathcal{F}$ *ein* τ*-Rahmen und* V *eine Abbildung ist, die jede Variable* $p \in \mathsf{VAR}$ *auf die Menge der Welten* $W_p \subseteq W$ *abbildet, in denen* p *gilt.*

Werden die Relationen bei der Angabe eines Kripke-Rahmens explizit aufgezählt, lassen wir die Mengenklammern der Einfachheit halber weg, z.B. schreiben wir für den Kripke-Rahmen $\mathcal{F} = (W, \{R\})$ für die einfache Modallogik auch $\mathcal{F} = (W, R)$.

Die in dieser Arbeit verwendete Definition von Erfüllbarkeit bedarf in Abgrenzung zur einfachen Modallogik nur noch einer Ergänzung für die neu eingeführten allgemeineren Konnektoren. Die sonstige Terminologie, insbesondere für Erfüllbarkeit etc. entspricht dem Grundstudium.

Definition 2.7. *Für eine modale Basis* $\tau = (O, \rho)$ *mit* $O = \{\triangle_1, \ldots, \triangle_n\}$ *und ein* τ*-Modell* $\mathcal{M} = (W, \{R_{\triangle_i} \mid \triangle_i \in O\}, V)$*,* $i \in \{1, \ldots, n\}$*, sagen wir, die Welt* $w \in W$ *erfüllt* $\triangle_i(\phi_1, \ldots, \phi_{\rho(\triangle_i)})$*, geschrieben* $\mathcal{M}, w \models \triangle_i(\phi_1, \ldots, \phi_{\rho(\triangle_i)})$*, g.d.w.*

$$\exists (w, v_1, \ldots, v_{\rho(\triangle_i)}) \in R_{\triangle_i} \text{ mit } \mathcal{M}, v_1 \models \phi_1, \ldots, \mathcal{M}, v_{\rho(\triangle_i)} \models \phi_{\rho(\triangle_i)}.$$

Die Formel $\triangle(\phi_1, \ldots, \phi_n)$ ist also in einer Welt w erfüllt, wenn es ein Tupel von Nachfolgerwelten von w gibt, sodass die j-te Komponente stets die j-te an $\triangle$ übergebene Formel erfüllt.

Beispiel 2.8

Sei $\tau = (\{\triangle, \square\}, \rho)$ und $\rho(\triangle) = 2, \rho(\square) = 3$. Wir wollen mit $\triangle$ Dreiecke modellieren und mit $\square$ Quadrate. Eine entsprechende Kripke-Struktur über $\mathsf{VAR} = \{r\}$ ist im Folgenden graphisch dargestellt, wobei links nur die Kanten für $\triangle$ und rechts nur die Kanten für $\square$ eingezeichnet sind. $V(r)$ sind alle rot eingezeichneten Welten. Es gelte $(u, v, w) \in R_\triangle$ genau dann wenn ein einfarbiges Dreieck mit den Eckpunkten u, v, w existiert. $R_\square$ wird analog konstruiert.

Es sei $\top = r \vee \neg r$ die wahre Aussage. Die Formel $r \wedge \triangle(r, r) \rightarrow \square(\top, \top, \top)$ ist nun für eine Welt erfüllt, falls daraus, dass sie Teil eines Dreiecks mit ausschließlich roten Eckpunkten ist, folgt, dass sie auch Teil eines Quadrats ist. Die Formel ist in allen Welten außer der Welt unten rechts erfüllt.

Dieses Beispiel ist inspiriert durch [1].

Je nach beabsichtigter Semantik können Einschränkungen wie zum Beispiel die Einschränkung erlaubter Rahmen sinnvoll sein. Wir betrachten dazu beispielhaft die modale Basis $\mathsf{TL} = (\{F, P\}, \rho), \rho(F) = \rho(P) = 1$, deren beabsichtigter Zweck es ist, Aussagen über die Zeit zu machen, wobei F für Ereignisse *irgendwann in der Zukunft* und P für Ereignisse *irgendwann in der Vergangenheit* steht [1].

Als Zeitpunkte können natürlich die Welten eines Kripke-Modells interpretiert werden, allerdings mit der Einschränkung, dass es möglich sein muss, die Welten in eine zeitliche Reihenfolge zu bringen, um die eindimensionale Zeit entsprechend abzubilden.

In der Modallogik, die wir bisher definiert haben, können ohne Einschränkung der Rahmen keine Aussagen der Form „irgendwann in der Zukunft" getroffen werden, da z.B. der nicht transitive Rahmen $\mathcal{F} = (\{0, 1, 2\}, \{(0, 1), (1, 2)\})$ zulässt, dass in 2 eine Aussage stimmt, die von 0 aus nicht direkt gesehen werden kann. Eine Semantik wie für F lässt sich nicht allgemein modellunabhängig formulieren, ohne unendliche Formeln wie $p \vee \Diamond p \vee \Diamond\Diamond p \vee \ldots$ zu verwenden. Wir schränken die für die Auswertung von TL-Formeln zugelassenen Rahmen daher so ein, dass sie einen linearen Zeitstrang modellieren.

Definition 2.9. *Es sei A eine Menge und $< \subset A \times A$ eine Relation auf A. Wir nennen $<$ eine Ordnungsrelation auf A g.d.w. $<$ transitiv, irreflexiv und zusammenhängend ist, d.h. für alle $a, b \in A$ gilt $a = b$ oder $(a, b) \in <$ oder $(b, a) \in <$.*

Ein Rahmen $\mathcal{F} = (W, R_F, R_P)$ für die temporale Logik muss, um die oben genannten Anforderungen zu erfüllen, die folgenden Eigenschaften haben:

- R_F ist eine Ordnungsrelation auf W
- $R_P = \{(u, v) \mid (v, u) \in R_F\}$

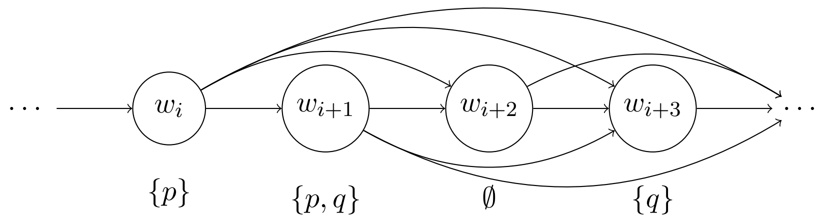
An dieser Stelle sei angemerkt, dass wir durch diese Definition keine Verzweigungen, wie man sie z.B. in Berechnungsbäumen finden könnte, erlauben. Zudem hat die so definierte Logik einige erhebliche Mängel, die wir im folgenden Beispiel sehen werden.

Beispiel 2.10

Herr Meier möchte umziehen. Eine Reihe von Gegenständen muss dafür von der alten Wohnung in ein Auto transportiert werden. Es sei W die Menge dieser Gegenstände und $\mathcal{M} = (W, R_F, R_P, V)$. Die Gegenstände sind unterschiedlich groß und für einen Gegenstand $w \in W$ gilt $w \in V(p)$ genau dann, wenn zum Tragen mehrere Personen benötigt werden sowie $w \in V(q)$ genau dann, wenn das Auto nach dem Einpacken des Gegenstandes nicht mit weiteren Gegenständen beladen werden kann, etwa weil der Gegenstand zerbrechlich ist oder weil es sich um den letzten Gegenstand handelt.

Wir nehmen an, dass die Gegenstände in einer bestimmten Reihenfolge in das Auto geladen werden müssen. Sei R so definiert, dass $(w_1, w_2) \in R_F$ für $w_1, w_2 \in W$ genau dann wenn w_2 nach w_1 eingepackt werden muss. Die Struktur R_P folgt dann aus der vorherigen Einschränkung für TL-Rahmen.

Ein Ausschnitt aus dem entstehenden Modell könnte folgendermaßen aussehen:



Herr Meier interessiert sich nun dafür, ob er zukünftig nochmal die Hilfe eines Freundes beim Umziehen benötigt und kann das durch das Auswerten der Formel Fp herausfinden. Mit der Formel $P(p \wedge q)$ kann z.B. herausgefunden werden, ob schon ein Gegenstand transportiert wurde, der so groß war, dass ein Helfer benötigt wurde und er das ganze Auto verstopft hat, während $\neg P(\neg q)$ gilt, falls bisher mit jeder Fahrt nur ein Gegenstand transportiert wurde.

Dieses Modell hat einige Grenzen: Leider kann Herr Meier nicht herausfinden, ob er für *den nächsten* Gegenstand einen Helfer benötigt. Ebenfalls gibt es keine Formel, die ihm sagt, ob er bis zum nächsten Losfahren noch Hilfe benötigt, d.h. ob bis zum nächsten Auftreten von q die Formel $\neg p$ gilt.

Außerdem sieht man, dass bereits für diesen kleinen Ausschnitt durch die Transitivität ein sehr unübersichtlicher Graph entsteht, obwohl wir auch allein durch die Kanten der Form (w_i, w_{i+1}) die Reihenfolge, in der die Gegenstände eingeladen werden müssen, eindeutig festlegen könnten.

Sollte die Liste der Gegenstände nicht enden, etwa weil Herr Meier schneller einkauft als er Gegenstände in die neue Wohnung transportieren kann, finden wir dann allerdings keine endliche Formel, die äquivalent zu $F\phi$ für ein $\phi \in \mathsf{TL}$ ist.

Im Folgenden sind die genannten Modallogik-Varianten und jeweils die dazugehörige modale Basis zusammengefasst:

Variante	**modale Basis** τ
Einfache Modallogik	$\mathsf{ML} := (\{\Diamond\}, \rho), \rho(\Diamond) = 1$
Multi-Modallogik	$(\{\Diamond_1, \dots, \Diamond_n\}, \rho), \rho(\Diamond_i) = 1 \; \forall i \in \{1, \dots, n\}$
Temporale Logik	$\mathsf{TL} := (\{F, P\}, \rho), \rho(F) = \rho(P) = 1$

Tabelle 2.1: Ausgewählte Modallogik-Varianten

2.3 Computation Tree Logic

Um die Aussagekraft der temporalen Logik von Einschränkungen für Modelle in die Definition der Logik selbst zu verlagern, bedient sich ein großes Teilgebiet der temporalen Logik, die Familie der *Computation Tree Logics*, zusätzlich zur bereits eingeführten Auswertung von Formeln abhängig von Nachfolgerwelten der Möglichkeit, Formeln über ganze Pfade auszuwerten.

Für eine Relation $R \subseteq W \times W$ heißt $x = x_0, x_1, \dots$ ein Pfad, falls $w_i \in W$ und $(w_i, w_{i+1}) \in R$ für alle $i \in \mathbb{N}$. Es bezeichne außerdem x^i den Suffix $x_i, x_{i+1}, \dots$.

Die folgenden Definitionen orientieren sich an [2] und [5]. Wir wollen zwei Varianten einführen, LTL und CTL. Als Vorbereitung definieren wir zunächst Syntax und Semantik der allgemeineren Variante CTL^*, die sowohl LTL als auch CTL enthält. Mit CTL^* können durch die nun zugelassenen Verzweigungen schließlich auch Berechnungsbäume analysiert werden.

Definition 2.11 (CTL*). *Es sei* VAR *eine endliche Menge von Variablen.* $\mathsf{FORM}_{\mathsf{CTL}^*}$*-Formeln lassen sich unterteilen in Zustandsformeln und Pfadformeln. Wir definieren* $\mathsf{FORM}_{\mathsf{CTL}^*}$ *rekursiv wie folgt:*

- *Für alle* $p \in \mathsf{VAR}$ *ist* p *eine Zustandsformel.*
- *Für Zustandsformeln* $\phi, \psi \in \mathsf{FORM}_{\mathsf{CTL}^*}$ *und Pfadformeln* π, χ *gilt:*
  1. $\neg\phi$, $(\phi \wedge \psi)$ *und* A_χ *sind Zustandsformeln.*
  2. $\phi, \neg\chi, (\chi \wedge \pi), X_\chi$ *und* $[\chi$ *until* $\pi]$ *sind Pfadformeln.*

CTL^**-Formeln werden auf Kripke-Strukturen für die einfache Modallogik ausgewertet. Die Semantik für* CTL^* *ist wie folgt definiert:*

Seien $\mathcal{M} = (W, R, V), p \in \mathsf{VAR}$ *und* $w \in W$ *sowie* ϕ, ψ *Zustandsformeln und* χ, π *Pfadformeln. Formeln können entweder auf Pfaden oder in Welten ausgewertet werden. In Welten können die folgenden Formeln ausgewertet werden:*

- $\mathcal{M}, w \models p$ *genau dann, wenn* $w \in V(p)$
- $\mathcal{M}, w \models \neg\phi$ *genau dann, wenn* $\mathcal{M}, w \not\models \phi$
- $\mathcal{M}, w \models \phi \wedge \psi$ *genau dann, wenn* $\mathcal{M}, w \models \phi$ *und* $\mathcal{M}, w \models \psi$
- $\mathcal{M}, w \models A_\chi$ *genau dann, wenn für alle in* w *beginnenden Pfade* $x = x_0, x_1, \dots$ *gilt:* $\mathcal{M}, x \models \chi$

Im Folgenden sei $x = (x_0, x_1, \dots)$ *ein Pfad. Die Gültigkeit von Pfadformeln ist definiert durch:*

- $\mathcal{M}, x \models \phi$ *genau dann, wenn* x *in einer Welt* $w = x_0$ *beginnt, sodass* $\mathcal{M}, w \models \phi$
- $\mathcal{M}, x \models \neg\chi$ *genau dann, wenn* $\mathcal{M}, x \not\models \chi$
- $\mathcal{M}, x \models \pi \wedge \chi$ *genau dann, wenn* $\mathcal{M}, x \models \pi$ *und* $\mathcal{M}, x \models \chi$
- $\mathcal{M}, x \models [\chi \textit{ until } \pi]$ *genau dann, wenn* $\mathcal{M}, x^k \models \pi$ *für ein* $k \geq 0$ *und* $\mathcal{M}, x^j \models \chi$ *für alle* $0 \leq j < k$
- $\mathcal{M}, x \models X_\chi$ *genau dann, wenn* $\mathcal{M}, x_1 \models \chi$ *gilt.*

Der Operator X erinnert dabei an die Box aus der bereits eingeführten Modallogik, kann jedoch nicht in Welten ausgewertet werden, während $AX_\varphi \Leftrightarrow \Box\varphi$ gilt. Auch ein Äquivalent zum Diamanten lässt sich finden: Analog zur einfachen Modallogik führen wir dazu $E_\varphi := \neg A_{\neg\varphi}$ ein. Dann gilt $EX_\varphi \Leftrightarrow \Diamond\varphi$. Zudem lässt sich der F-Operator der einfachen temporalen Logik imitieren durch [**true** until φ]. Für $\varphi \in \mathsf{FORM}_{\mathsf{CTL}^*}$ schreiben wir $G\varphi$ als Abkürzung für $\neg F\neg\varphi$.

2.3.1 CTL

In der Regel interessiert man sich vor allem für die Gültigkeit von Formeln in bestimmten Zuständen der Berechnung, sodass in der Praxis in der Regel nicht die Logik CTL^* verwendet wird, sondern z.B. die Logik CTL, die eine Teilmenge von CTL^* ist. Ebenfalls führen wir die lineare temporale Logik LTL ein, die ebenfalls eine Teilmenge von CTL^* ist. Die Definitionen für die Gültigkeit einer Formel auf einem Pfad werden in CTL nicht mehr explizit benötigt, sondern in der Semantik der erlaubten Operatoren versteckt.

Definition 2.12 (CTL)**.** *Es sei* VAR *eine endliche Menge von Variablen. Dann ist* $\mathsf{FORM}_{\mathsf{CTL}}$ *folgendermaßen definiert:*

- $p \in \mathsf{FORM}_{\mathsf{CTL}}$ *für alle* $p \in \mathsf{VAR}$
- *Für* $\phi, \psi \in \mathsf{FORM}_{\mathsf{CTL}}$ *gilt:*
  (1) $\neg\phi \in \mathsf{FORM}_{\mathsf{CTL}}$
  (2) $\phi \wedge \psi \in \mathsf{FORM}_{\mathsf{CTL}}$
  (3) $AX\phi \in \mathsf{FORM}_{\mathsf{CTL}}$
  (4) $A[\phi \textit{ until } \psi] \in \mathsf{FORM}_{\mathsf{CTL}}$

Dabei ist $A[\phi \text{ until } \psi]$ bei Auswertung in einer Welt w zu lesen als „Für alle von w ausgehenden Pfade gilt solange ϕ, bis ψ gilt“ und $AX\phi$ als „In allen direkten Nachfolgerwelten von w gilt ϕ“.

Beispiel 2.13

Wir betrachten ein zugbasiertes Strategiespiel, in dem der Spieler eine gewisse Abfolge von Aktionen ausführen muss, um zum Erfolg zu kommen, und eine Variablenmenge $\mathsf{VAR} = \{\mathsf{success}, \mathsf{init}, \mathsf{mission}\}$. Für einen Zustand des Spiels gelte

- $\mathsf{success}$, falls die Herausforderung erfolgreich abgeschlossen wurde,
- init, falls es sich um den Ausgangszustand handelt,
- $\mathsf{mission}$, falls eine Zwischenmission bereits erledigt wurde.

Es sei nun $\mathcal{M} = (W, R, V)$ ein Modell, wobei W die Menge der möglichen Spielsituationen ist und $(w_1, w_2) \in R$ genau dann, wenn der Spieler die Situation w_2 durch eine einzelne Aktion in w_1 herbeiführen kann. Die folgenden Anforderungen an das Spiel können mittels CTL formuliert werden:

- $\varphi_1 := \mathsf{init} \to EF\mathsf{success}$ (Das Spiel soll lösbar sein, d.h. vom Startzustand aus soll eine Aktionenfolge existieren, die zum Erfolg führt.)
- $\varphi_2 := E[\neg\mathsf{mission}\ \text{until}\ \mathsf{success} \wedge \mathsf{mission}]$ (Es gibt einen Weg, das Spiel zu gewinnen, bei dem erst im letzten Zug die Zwischenmission erledigt wird.)
- $\varphi_3 := AF\mathsf{mission}$ (Die Zwischenmission ist nach einer endlichen Anzahl an Schritten erfolgreich abgeschlossen, egal wie der Spieler spielt.)

Aus technischen Gründen führen wir eine weitere Struktur ein, auf der CTL-Formeln ausgewertet werden können, sogenannte Hintikka-Strukturen. Der wesentliche Unterschied ist, dass die Funktion V, die jeder Variablen die Welten zuordnet, in denen sie gilt, durch eine Funktion L ersetzt wird, die eine Welt auf in ihr geltende Formeln abbildet. Um eine Analogie zu den bereits eingeführten Modellen zu erhalten, führen wir eine Reihe von Axiomen ein, die die Konsistenz der Funktion L gewährleisten sollen.

Definition 2.14 (Hintikka-Struktur)**.** *Eine Hintikka-Struktur ist ein Tupel $\mathcal{M} = (W, R, L)$, sodass L für alle $w \in W$ und $\phi, \psi \in \mathsf{FORM}_{\mathsf{CTL}}$ die folgenden Eigenschaften erfüllt:*

(H1) $\neg\phi \in L(w) \Rightarrow \phi \notin L(w)$

(H2) $\neg\neg\phi \in L(w) \Rightarrow \phi \in L(w)$

(H3) $\phi \wedge \psi \in L(w) \Rightarrow \phi \in L(w), \psi \in L(w)$

(H4) $\neg(\phi \wedge \psi) \in L(w) \Rightarrow \neg\phi \in L(w)$ *oder* $\neg\psi \in L(w)$

(H5) $A[\phi\ \mathit{until}\ \psi] \in L(w) \Rightarrow \psi \in L(w)$ *oder* $\phi, AXA[\phi\ \mathit{until}\ \psi] \in L(w)$

(H6) $\neg A[\phi\ \mathit{until}\ \psi] \in L(w) \Rightarrow \neg\phi, \neg\psi \in L(w)$ *oder* $\neg\psi, \neg AXA[\phi\ \mathit{until}\ \psi] \in L(w)$

(H7) $AX\phi \in L(w) \Rightarrow$ *für alle v mit $(w, v) \in R$ gilt $\phi \in L(v)$.*

(H8) $\neg AX\phi \in L(w) \Rightarrow$ *es existiert ein v mit $(w, v) \in R$ und $\neg\phi \in L(v)$.*

(H9) $A[\phi\ \mathit{until}\ \psi] \in L(w) \Rightarrow$ *für alle Pfade $x = x_0, x_1, x_2, \ldots,$ die in $w = x_0$ beginnen, gibt es ein $i \geq 0$, sodass $\psi \in L(x_i)$ und $\phi \in L(x_j)$ für $0 \leq j < i$.*

Man beachte, dass sich durch die Definition von $E\varphi$ und $F\varphi$ als Abkürzungen für $\neg A\neg\varphi$ bzw. [**true** until φ] das Axiomensystem im Vergleich zu [2] deutlich vereinfacht. $(H9)$ beinhaltet zudem das Axiom $(H5)$, allerdings werden wir später die strikte Trennung benötigen. Dass Hintikka-Strukturen konsistent mit den vorher eingeführten Modellen sind, beweist das folgende Lemma:

Lemma 2.15. *Jede Hintikka-Struktur (W, R, L) kann zu einem Modell $\mathcal{M} = (W, R, V)$ erweitert werden, sodass*

$$(*)\ \varphi \in L(w) \Rightarrow \mathcal{M}, w \models \varphi \text{ für alle } w \in W.$$

Für jedes Modell $\mathcal{M} = (W, R, V)$ ist $(W, R, w \mapsto \{\varphi \in \mathsf{FORM_{CTL}} \mid \mathcal{M}, w \models \varphi\})$ eine Hintikka-Struktur. Wir nennen $\mathcal{M}'$ auch die kanonische Hintikka-Struktur *von $\mathcal{M}$.*

Beweis. Die zweite Aussage ist offensichtlich, da die Gültigkeit der Axiome direkt aus der Definition der Semantik von CTL folgt. Wir zeigen daher nur den ersten Teil.

Sei VAR eine Variablenmenge. Wir setzen $V(p) := \{w \in W \mid p \in L(w)\}$ für alle $p \in \mathsf{VAR}$. Wir zeigen nun durch eine Induktion über φ, dass für $\mathcal{M} = (W, R, V)$ bereits $(*)$ erfüllt ist. Aus technischen Grunden müssen wir zusätzlich für alle φ die folgende Aussage zeigen:

$$(**)\ \neg\varphi \in L(w) \Rightarrow \mathcal{M}, w \models \neg\varphi \text{ für alle } w \in W.$$

(I.A.) Nach Konstruktion von V gilt für alle $p \in \mathsf{VAR}$: $p \in L(w) \Leftrightarrow w \in V(p) \Leftrightarrow \mathcal{M}, w \models p$.

Ebenfalls gilt $\neg p \in L(w) \overset{(H1)}{\Rightarrow} p \notin L(w) \Leftrightarrow w \notin V(p) \Leftrightarrow \mathcal{M}, w \not\models p \Leftrightarrow \mathcal{M}, w \models \neg p$.

(I.S.) Es gelte $(*)$ und $(**)$ für $\phi, \psi \in \mathsf{FORM_{CTL}}$ und deren Teilformeln (Induktionsvoraussetzung). Wir zeigen $(*)$ und $(**)$ für die folgenden Formeln:

(1) $\underline{\neg\phi}$

Die Gültigkeit von $(*)$ folgt direkt nach Induktionsvoraussetzung. Wir nehmen also an, dass $\neg\neg\phi \in L(w)$. Mit $(H2)$ folgt $\phi \in L(w)$ und mit Anwendung der Induktionsvoraussetzung $\mathcal{M}, w \models \phi \Leftrightarrow \mathcal{M}, w \models \neg\neg\phi$.

(2) $\underline{\phi \wedge \psi}$

Zeige zunächst $(*)$: Mit (H3) folgt $\phi \in L(w)$ und $\psi \in L(w)$. Nach Induktionsvoraussetzung gilt dann $\mathcal{M}, w \models \phi$ und $\mathcal{M}, w \models \psi$ und folglich $\mathcal{M}, w \models \phi \wedge \psi$.

Für $\neg(\phi \wedge \psi) \in L(w)$ folgt mit $(H4)$, dass $\neg\phi \in L(w)$ oder $\neg\psi \in L(w)$. Wendet man die Induktionsvoraussetzung an, erhält man $\mathcal{M}, w \models \neg\phi$ oder $\mathcal{M}, w \models \neg\psi$. Es gilt also in jedem Fall $\mathcal{M}, w \not\models \phi$ oder $\mathcal{M}, w \not\models \psi$ und damit $\mathcal{M}, w \not\models \phi \wedge \psi \Leftrightarrow \mathcal{M}, w \models \neg(\phi \wedge \psi)$.

(3) $\underline{A[\phi \text{ until } \psi]}$

Aus $A[\phi \text{ until } \psi] \in L(w)$ folgt mit (H9), dass für alle Pfade $x = x_0, x_1, \ldots,$ die in $w = x_0$ beginnen, für ein $i \geq 0$ gilt: $\psi \in L(x_i)$ und $\phi \in L(x_j)$ für $0 \leq j < i$. Mit der Induktionsvoraussetzung gilt dann $\mathcal{M}, x_i \models \psi$ und $\mathcal{M}, x_j \models \phi$ für alle Pfade x von w. Nach Definition folgt damit direkt $\mathcal{M}, w \models A[\phi \text{ until } \psi]$.

Für $(**)$ gelte $\neg A[\phi \text{ until } \psi] \in L(w)$. $(H6)$ liefert, dass entweder $\neg\phi, \neg\psi \in L(w)$ oder $\neg\psi, \neg AXA[\phi \text{ until } \psi] \in L(w)$.

Wir zeigen, dass es einen Pfad $v_0, v_1, \ldots$ von $w = v_0$ gibt, sodass entweder $\neg\psi \in L(v_i)$ für alle i oder ein j existiert, sodass $\neg\phi \in L(v_j)$ und $\neg\psi \in L(v_k)$ für alle $k \leq j$. Dafür führen wir eine Induktion über die Länge dieses Pfades durch.

(I.A.) Mit $(H6)$ folgt in jedem Fall $\neg\psi \in L(w) = L(v_0)$, sodass der Pfad v_0 die Kriterien erfüllt.

(I.S.) Sei $v_0, \dots, v_k$ ein Pfad der gewünschten Form. Wir zeigen nun, dass dann auch ein Pfad $v_0, v_1, \dots, v_{k+1}$ dieser Form existiert.

Falls $\neg\phi \in L(v_i)$ für ein $i \leq k$, sind wir fertig. Ansonsten gilt insbesondere $\neg\phi \notin L(v_k)$, woraus mit $(H6)$ folgt: $\neg AXA[\phi \text{ until } \psi] \in L(v_k)$. Dann existiert durch $(H8)$ eine Welt v_{k+1} mit $(v_k, v_{k+1}) \in R$ und $\neg A[\phi \text{ until } \psi] \in L(v_{k+1})$. Schließlich liefert $(H6)$, dass $\neg\psi \in L(v_{k+1})$, woraus die Aussage folgt.

Falls es für $v_0, v_1, \dots$ nun ein i gibt mit $\mathcal{M}, v_i \models \psi$, dann muss wegen $\neg\psi \in L(v_i) \overset{\text{(IV)}}{\Rightarrow} \mathcal{M}, v_i \models \neg\psi$ gelten: $\neg\psi \notin L(v_i)$, d.h. nach obiger Behauptung muss es ein $j < i$ geben, sodass $\neg\phi, \neg\psi \in L(v_j)$ und folglich $\mathcal{M}, v_j \models \neg\phi, \mathcal{M}, v_j \models \neg\psi$.

Nach der Definition von $\models$ folgt schließlich, dass $\mathcal{M}, w \not\models A[\phi \text{ until } \psi] \Leftrightarrow \mathcal{M}, w \models \neg A[\phi \text{ until } \psi]$.

(4) $\underline{AX\phi}$

Aus $AX\phi \in L(w)$ folgt mit (H7), dass für alle $v \in W$ mit $(w, v) \in R$ gilt: $\phi \in L(v)$. Mit der Induktionsvoraussetzung folgt $\mathcal{M}, v \models \phi$, d.h für alle $(w, v) \in W$ gilt $\mathcal{M}, v \models \phi$. Daraus folgt $\mathcal{M}, w \models AX\phi$ nach Definition und damit $(*)$.

$\neg AX\phi \in L(w) \overset{\text{(H8)}}{\Rightarrow}$ es existiert ein v mit $(w, v) \in R$ und $\neg\phi \in L(v)$. Die Induktionsvoraussetzung liefert $\mathcal{M}, v \models \neg\phi$, woraus schließlich $\mathcal{M}, v \not\models \phi$ und damit $\mathcal{M}, w \not\models AX\phi$ folgt. Nach Definition folgt $\mathcal{M}, w \models \neg AX\phi$, wodurch $(**)$ folgt.

Nach der rekursiven Definition von $\mathsf{FORM}_{\mathsf{CTL}}$ gilt damit $(*)$ für alle $\varphi \in \mathsf{FORM}_{\mathsf{CTL}}$. □

2.3.2 LTL

Auch in der linearen temporalen Logik interessiert man sich für Berechnungen von Programmen und die Gültigkeit von Formeln zu gewissen Zeitpunkten dieser Berechnung. Der wesentliche Unterschied ist, dass LTL keine Verzweigungen in den Berechnungen zulässt, was zu den für CTL namensgebenden Berechnungsbäumen führen würde, sondern stattdessen Formeln auf einem einzelnen Berechnungspfad auswertet.

Definition 2.16 (LTL)**.** *Es sei* VAR *eine endliche Menge von Variablen. Dann ist* $\mathsf{FORM}_{\mathsf{LTL}}$ *folgendermaßen definiert:*

- $p \in \mathsf{FORM}_{\mathsf{LTL}}$ *für alle* $p \in \mathsf{VAR}$
- *Für* $\phi, \psi \in \mathsf{FORM}_{\mathsf{LTL}}$ *gilt:*
  (1) $\neg\phi \in \mathsf{FORM}_{\mathsf{LTL}}$
  (2) $\phi \wedge \psi \in \mathsf{FORM}_{\mathsf{LTL}}$
  (3) $X_\phi \in \mathsf{FORM}_{\mathsf{LTL}}$
  (4) $[\phi \text{ until } \psi] \in \mathsf{FORM}_{\mathsf{LTL}}$

Da sowohl die durch (3) als auch die durch (4) erzeugten Formeln nach CTL*-Definition auf Pfaden statt auf Welten ausgewertet werden, sehen die Modelle für LTL etwas anders als die für CTL aus. Weil Formeln sowieso nur auf einem einzelnen Pfad ausgewertet werden, benötigen wir keinen Kripke-Rahmen zur Auswertung, sondern ersetzen diesen durch einen Pfad.

Für einen Pfad $x = x_0, x_1, \ldots$ ist implizit

$$W = \{x_i \mid i \in \mathbb{N}\} \text{ und } R = \{(w_i, w_{i+1}) \mid i \in \mathbb{N}\}.$$

LTL-Modelle sind somit der Form

$$\pi = (x, V),$$

wobei $V\colon \mathsf{VAR} \to \mathcal{P}(W)$ wie gewohnt definiert ist. Wir schreiben für $\varphi \in \mathsf{FORM}_{\mathsf{LTL}}$ nun

$$\pi, i \models \varphi \text{ genau dann wenn } (x^i, V) \models \varphi.$$

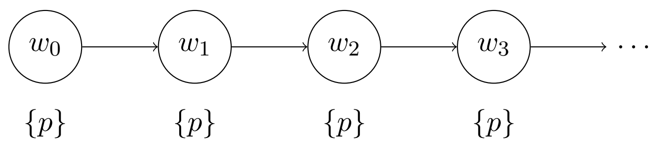
2.4 Endliche Modelleigenschaft

Abschließend soll in diesem Kapitel definiert werden, was es für eine Modallogik-Variante heißt, die endliche Modelleigenschaft zu besitzen.

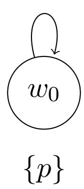
Beispiel 2.17

Wir betrachten die modallogische Formel $\varphi = \Diamond p$, die für eine Welt prüft, ob sie eine Nachfolgerwelt besitzt, in der p gilt sowie das Modell $\mathcal{M} = (W, R, V)$, wobei

$$W = \{w_i \mid i \in \mathbb{N}\}, R = \{(w_i, w_{i+1}) \mid i \in \mathbb{N}\}, V(p) = W.$$



Offenbar gilt $\mathcal{M} \models \varphi$, da jede Welt eine Nachfolgerwelt besitzt, in der p gilt. Dieses Modell besitzt unendlich viele Welten, die für die Erfüllung der Formel jedoch keineswegs nötig sind, denn ein kleineres Modell, in dem jede Welt einen Nachfolger hat, wäre z.B. das folgende:



$\mathcal{M}' = (\{w_0\}, \{(w_0, w_0)\}, V')$, wobei $V'(p) = \{w_0\}$.

Offenbar gilt auch $\mathcal{M}', w_0 \models \phi$, jedoch kommt das Modell nun mit einer endlichen Anzahl von Welten aus; es genügt sogar eine einzige Welt.

Dieses und ähnliche Beispiele motivieren die Frage, ob eine solche Vereinfachung für beliebige Formeln möglich ist. Dadurch, dass mit den Operatoren $\Box$ und $\Diamond$ bei endlich häufiger Anwendung auch nur endlich weit geschaut werden kann, ist die Intuition, dass endlich viele Welten für die Erfüllung einer modallogischen Formel stets ausreichen sollten, sofern sie überhaupt erfüllbar ist. Diese Eigenschaft, dass jede erfüllbare Formel bereits mit einem endlichen Modell erfüllt werden kann, heißt endliche Modelleigenschaft. In Kapitel 3 werden wir zeigen, dass die einfache Modallogik tatsächlich die endliche Modelleigenschaft besitzt. Zunächst müssen wir allerdings präzisieren, was damit gemeint ist:

Definition 2.18 (Endliche Modelleigenschaft). *Es sei τ eine modale Basis. τ besitzt die endliche Modelleigenschaft, falls alle erfüllbaren $\phi \in \mathsf{FORM}_\tau$ auch auf einem endlichen Modell erfüllbar sind.*

Auf LTL kann diese Definition übertragen werden, indem man fordert, dass jede erfüllbare Formel auch auf einem endlichen Pfad erfüllbar sein muss, während die Definition für CTL exakt der Definition gleicht.

In diesem Kontext führen wir auch den Begriff der modalen Tiefe ein, der uns zeigt, wie lang die Pfade, die wir von einer Welt ausgehend verfolgen müssen, um eine Formel (einfacher Modallogik) auszuwerten, maximal sind. Tatsächlich lässt sich durch den endlichen Grad einer Formel auch argumentieren, dass die Anzahl der für die Formel überhaupt relevanten sichtbaren Welten endlich ist. Dieses Argument wird in Kapitel 3 vertieft, wenn die Konstruktion endlicher Teilmodelle durch Bisimulationen untersucht wird.

Definition 2.19 (Modale Tiefe). *Es sei* VAR *eine Menge von Variablen und $\tau = (O, \rho)$ eine modale Basis. Die modale Tiefe einer Formel $\varphi \in \mathsf{FORM}_\tau$, geschrieben $d(\varphi)$ ist rekursiv definiert durch:*

- $d(p) = 0$ *für alle* $p \in \mathsf{VAR}$
- $d(\neg\varphi) = d(\varphi)$
- $d(\phi \wedge \psi) = \max\{d(\phi), d(\psi)\}$
- $d(\triangle(\phi_1, \ldots, \phi_n)) = 1 + \max\{d(\phi_1), \ldots, d(\phi_n)\}$ *für alle* $\triangle \in O$ *mit* $\rho(\triangle) = n$.

Beispiel 2.20

Die Formel $\varphi := \Box\Diamond p \wedge \Box p$ hat eine modale Tiefe von 2; es gilt $d(\varphi) = 2$.

$$\underbrace{\underbrace{\Box \underbrace{\Diamond p}_{d=1}}_{d=2} \wedge \underbrace{\Box p}_{d=1}}_{d=\max\{2,1\}=2}$$

Soll die Formel in w_1 des Modells aus Beispiel 2.4 ausgewertet werden, sind die Welten w_4, w_5 usw. nicht sichtbar, weil der kürzeste von w_1 zu ihnen führende Pfad eine Länge von $3 > d(\varphi)$ hat. Die Existenz dieser Welten beeinflusst die Gültigkeit von φ in w_1 somit nicht.

3 Einfache Modallogik

In diesem Kapitel werden wir zeigen, dass die Modallogik für beliebige modale Basen die endliche Modelleigenschaft besitzt. Wir werden dafür zunächst die Methode der Filtrierung wie in [1] einführen und sie nutzen, um endliche Quotientenmodelle zu erzeugen, die bestimmte Strukturen, für die wir uns interessieren, beibehalten. Anschließend werden wir zeigen, dass die Filtrierung alle Anforderungen erfüllt, die wir zum Nachweis der endlichen Modelleigenschaft einfacher modaler Logik benötigen.

Diese Ergebnisse aus [1] verallgemeinern wir im zweiten Teil für alle modalen Basen, die nur unäre Konnektoren einführen (Multi-Modallogik). Dafür ist nur eine kleine Anpassung der Filtrierung notwendig und die Argumentation funktioniert analog zur einfachen Modallogik.

Natürlich beeinflusst die endliche Modelleigenschaft auch Erfüllbarkeitsprobleme für die Modallogik. Wir werden die konkrete obere Schranke für die Größe eines minimalen Modells für eine gegebene Formel ausnutzen, um einen naiven Brute-Force-Algorithmus zu konstruieren, der die einfache Modallogik entscheidet. Das Erfüllbarkeitsproblem formulieren wir durch die folgende Definition.

Definition 3.1. *Die Sprache* $\mathsf{ModalSAT}$ *ist die Menge*

$$\{\varphi \in \mathsf{FORM}_{\mathsf{ML}} \mid \exists\, \mathcal{M} = (W, R, V) \text{ sodass für ein } w \in W \text{ gilt: } \mathcal{M}, w \models \varphi\}$$

aller erfüllbaren modallogischen Formeln.

Für die Modallogik lassen sich verschiedene Rahmenklassen wie in [4] einführen (wir verzichten auf eine formale Definition), mit denen sich die Menge der möglichen Modelle einschränken lässt. Rahmenklassen haben einerseits Auswirkungen auf die Erfüllbarkeit von Formeln (z.B. ist $p \wedge \neg\Diamond p$ für reflexive Rahmen nicht erfüllbar), andererseits auch auf die endliche Modelleigenschaft. Mit Fokus auf dem zweitgenannten Aspekt untersuchen wir beispielorientiert und ohne Anspruch auf Vollständigkeit, welche Eigenschaften die Filtrierung beibehält.

Schließlich betrachten wir eine Möglichkeit, die endliche Modelleigenschaft auch für mehrdimensionale Konnektoren zu zeigen, die im Wesentlichen auf einer leicht abgewandelten Version von Bisimulationen aufbaut. Die entsprechende Argumentation für den Fall unärer Konnektoren ist ebenfalls in [1] zu finden.

3.1 Eindimensionale Konnektoren

3.1.1 Einfache Modallogik

Das Konzept der Filtrierung ist motiviert durch die Quotientengruppen aus der Gruppentheorie, die uns erlauben, Gruppen so zu vereinfachen, dass wir für uns irrelevante Merkmale eliminieren können. Die Quotientengruppe $\mathbb{Z}/2\mathbb{Z}$ eliminiert z.B. Vielfache von 2, da wir uns nur für den Rest interessieren. Wir erreichen das durch die Definition von Äquivalenzklassen bzgl. eines gewissen Merkmals, hier also

$$a \sim b :\Leftrightarrow a \equiv b \mod 2.$$

Insbesondere ist die Quotientengruppe selbst eine Gruppe (bestehend aus den Äquivalenzklassen), sie erhält also die grundlegenden strukturellen Eigenschaften.

Die Filtrierung führt eine Äquivalenzrelation ein, die die Welten eines Modells danach einteilt, welche Formeln einer Formelmenge Φ in ihnen erfüllt sind. Die strukturelle Eigenschaft, an deren Beibehaltung wir interessiert sind, ist in diesem Kontext die Gültigkeit von Formeln aus Φ.

Im einfachsten Fall, dass $\Phi = \{p\}$ für eine Variable p ist, erhalten wir damit für $\mathcal{M} = (W, R, V)$ zwei Äquivalenzklassen, nämlich $V(p)$ und $W \backslash V(p)$.

Ähnlich wie Normalteiler in der Gruppentheorie eine Rolle spielen, können wir ein vergleichbares Konzept für die Modallogik entwerfen – unter Teilformeln abgeschlossene Formelmengen ermöglichen später eine Induktion, mit der wir zeigen, dass die Gültigkeit von Formeln aus Φ beibehalten wird.

Definition 3.2 (Abschluss unter Teilformeln). *Es sei Φ eine Menge von Formeln. Φ heißt abgeschlossen unter Teilformeln, falls Folgendes gilt:*

- $\neg\phi \in \Phi \Rightarrow \phi \in \Phi$
- $\phi \wedge \psi \in \Phi \Rightarrow \phi \in \Phi$ *und* $\psi \in \Phi$
- $\triangle(\phi_1, \ldots, \phi_n) \in \Phi \Rightarrow \phi_1, \ldots, \phi_n \in \Phi$

Für eine Formel φ bezeichnet $\mathsf{sub}(\varphi)$ den Durchschnitt aller unter Teilformeln abgeschlossenen Mengen, die φ enthalten.

Definition 3.3 (Filtrierung). *Es sei $\mathcal{M} = (W, R, V)$ ein Modell für die einfache Modallogik und Φ abgeschlossen unter Teilformeln. Dann definieren wir die Äquivalenzrelation $\sim_\Phi$ auf W wie folgt:*

$$w \sim_\Phi v \text{ g.d.w. } \mathcal{M}, w \models \varphi \Leftrightarrow \mathcal{M}, v \models \varphi \text{ für alle } \varphi \in \Phi$$

Für $w \in W$ schreiben wir $|w|_\Phi$ für $\{v \in W \mid v \sim_\Phi w\}$ und $W_\Phi = \{|w|_\Phi \mid w \in W\}$. Ein Modell $\mathcal{M}^f_\Phi = (W^f, R^f, V^f)$ heißt Filtrierung von $\mathcal{M}$ über Φ, falls

(1) $W^f = W_\Phi$

(2) $(|w|_\Phi, |v|_\Phi) \in R^f$ *für alle* $(w, v) \in R$ *(d.h. alle Verbindungen, die zwischen Welten im ursprünglichen Modell bestanden, müssen auch zwischen den entsprechenden Äquivalenzklassen bestehen)*

(3) Falls $(|w|_\Phi, |v|_\Phi) \in R^f$ *und* $\Diamond\phi \in \Phi$*, dann gilt* $\mathcal{M}, v \models \phi \Rightarrow \mathcal{M}, w \models \Diamond\phi$.

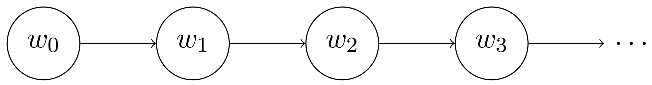
(4) Für jede in Φ vorkommende Variable p gilt $|w|_\Phi \in V^f(p)$ g.d.w. $\mathcal{M}, w \models p$.

Die dritte Anforderung an Filtrierungen wurde vor allem aus technischen Gründen formuliert, sie ist allerdings nicht notwendig, wenn wir die Forderung in (2) so verschärfen, dass für jede Kante $(|w|_\Phi, |v|_\Phi) \in R^f$ auch $w' \in |w|_\Phi, v' \in |v|_\Phi$ existieren müssen mit $(w', v') \in R$ (d.h. es dürfen nur dann Kanten zwischen zwei Äquivalenzklassen eingefügt werden, wenn zumindest eine Kante zwischen beliebigen Repräsentanten der jeweiligen Klassen besteht). Um das zu sehen, stellen wir zunächst fest, dass aus $\Diamond\phi \in \Phi$ auch $\phi \in \Phi$ folgen muss. Wenn wir nun eine Kante $(|w|_\Phi, |v|_\Phi) \in R^f$ der Form aus (3) betrachten, d.h. $\mathcal{M}, v \models \phi$, dann folgt für alle $v' \in |v|_\Phi$, dass $\mathcal{M}, v' \models \phi$. Aufgrund von $(|w|_\Phi, |v|_\Phi) \in R^f$ muss dann für ein $w' \in |w|_\Phi$ und ein $v' \in |v|_\Phi$ gelten: $(w', v') \in R$. Es ist leicht zu sehen, dass dann $\mathcal{M}, w' \models \Diamond\phi$ gelten muss und – wegen $\Diamond\phi \in \Phi$ – entsprechend auch $\mathcal{M}, w'' \models \Diamond\phi$ für alle $w'' \in |w|_\Phi$.

Beispiel 3.4

Es seien $\Phi = \{p_4, \Diamond p_4\}$ und $\mathcal{M} = (W, R, V)$ ein Modell über der Variablenmenge $\{p_k \mid k \in \mathbb{N}^*\}$ mit $W = \{w_i \mid i \in \mathbb{N}\}$, $V(p_k) = \{w_{kn} \mid n \in \mathbb{N}\}$ für alle $k \in \mathbb{N}^*$ und $R = \{(w_i, w_{i+1}) \mid i \in \mathbb{N}\}$.

Φ ist offenbar unter Teilformeln abgeschlossen.



Dann gilt $w \sim_\Phi v$ für $w, v \in W$, falls $\mathcal{M}, w \models p_4 \Leftrightarrow \mathcal{M}, v \models p_4$ und $\mathcal{M}, w \models \Diamond p_4 \Leftrightarrow \mathcal{M}, v \models \Diamond p_4$.

In jeder der Welten $w \in W$ gilt eine bestimmte Teilmenge der Formeln in Φ. Es gilt $\mathcal{P}(\Phi) = \{\emptyset, \{p_4\}, \{\Diamond p_4\}, \Phi\}$, es gibt also vier Möglichkeiten für jedes w, welche Formeln aus Φ in w gelten.

Es gilt

- $\mathcal{M}, w_{4k} \models p_4$ und $\mathcal{M}, w_{4k} \not\models \Diamond p_4$ für alle $k \in \mathbb{N}$
- $\mathcal{M}, w_{4k+3} \not\models p_4$ und $\mathcal{M}, w_{4k+3} \models \Diamond p_4$ für alle $k \in \mathbb{N}$
- $\mathcal{M}, w_{4k+i} \not\models p_4$ und $\mathcal{M}, w_{4k+i} \not\models \Diamond p_4$ für alle $k \in \mathbb{N}$ und $i \in \{1, 2\}$

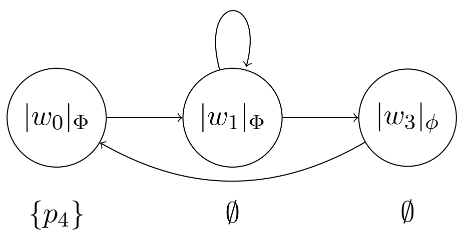
Tatsächlich gibt es also nur drei Äquivalenzklassen, sodass $W_\Phi = \{|w_0|_\Phi, |w_1|_\Phi, |w_3|_\Phi\}$ gilt.

Wir definieren das Modell $\mathcal{M}_\Phi^f = (W_\Phi^f, R^f, V^f)$ und gemäß (4) der Definition 3.3 setzen wir $V^f(p_4) = \{|w_0|_\Phi\}$. Für alle anderen Variablen p_k ist $V^f(p_k)$ beliebig, wir setzen also $V^f(p_k) = \emptyset$ für alle $4 \neq k \in \mathbb{N}^*$.

Zudem gilt $R^f = \{(|w_0|_\Phi, |w_1|_\Phi), (|w_1|_\Phi, |w_1|_\Phi), (|w_1|_\Phi, |w_3|_\Phi), (|w_3|_\Phi, |w_0|_\Phi)\}$, damit $\mathcal{M}^f$ (2) aus der Definition erfüllt ist (die Kanten zwischen den Welten in $\mathcal{M}$ übertragen sich auf die entsprechenden Äquivalenzklassen).

Prüfe nun, ob (3) gilt. Da $\mathcal{M}, w \models p_4 \Rightarrow |w|_\Phi = |w_0|_\Phi$, bleibt die Aussage nur für die einzige in $|w_0|_\Phi$ eingehende Kante $(|w_3|_\Phi, |w_0|_\Phi)$ zu zeigen. Für alle $w_{4n+3} \in W$, $n \in \mathbb{N}$ gilt aber $(w_{4n+3}, w_{4n+4}) \in R$. Da $w_{4n+4} = w_{4(n+1)}$, gilt aber $\mathcal{M}, w_{4n+4} \models p_4$, also auch $\mathcal{M}, w_{4n+3} \models \Diamond p_4$ und insbesondere $\mathcal{M}, w_{4n+4} \models p_4 \Rightarrow \mathcal{M}, w_{4n+3} \models \Diamond p_4$ für alle $n \in \mathbb{N}$.

Damit ist $\mathcal{M}_\Phi^f$ eine Filtrierung von $\mathcal{M}$ über Φ.



Für die Filtrierung aus dem letzten Beispiel kann schnell nachgeprüft werden, dass für alle $\varphi \in \Phi$ gilt: $\mathcal{M}, w \models \varphi \Leftrightarrow \mathcal{M}_\Phi^f, |w|_\Phi \models \varphi$. Ebenfalls haben wir im Beispiel gesehen, dass die Kardinalität der Potenzmenge von Φ die Anzahl der Äquivalenzklassen und damit auch die Größe der Filtrierung beschränkt.

Mit den beiden folgenden Lemmata zeigen wir, dass das letzte Beispiel kein Sonderfall ist und dass die genannten Eigenschaften stets gelten. Insbesondere existiert, falls $\mathcal{M}, w \models \varphi$ für eine Welt w des Modells $\mathcal{M}$ gilt, auch in jeder Filtrierung nach Φ mit $\varphi \in \Phi$ eine entsprechende Welt, in der φ erfüllt ist. Die endliche Modelleigenschaft folgt also direkt aus diesen beiden Eigenschaften (Satz 3.7).

Lemma 3.5. *Es sei $\mathcal{M} = (W, R, V)$ und Φ abgeschlossen unter Teilformeln mit $\varphi \in \Phi$. Dann gilt $\mathcal{M}^f_\Phi, |w|_\Phi \models \varphi \Leftrightarrow \mathcal{M}, w \models \varphi$.*

Beweis. Sei VAR die Menge der in Φ vorkommenden Variablen. Wir führen eine Induktion über die modale Tiefe der Formel φ durch.

(I.A.) $\underline{d(\varphi) = 0}$:

Wir zeigen die Behauptung durch Induktion über die Anzahl der Anwendungen von $\neg$ und $\wedge$.

(I.A.) Angenommen, φ enthält weder $\neg$ noch $\wedge$. Aus $d(\varphi) = 0$ folgt, dass $\varphi \in$ VAR. Sei also $\varphi = p$ für $p \in$ VAR. Nach (4) aus der Definition von $\mathcal{M}^f_\Phi$ gilt $\mathcal{M}, w \models p$ g.d.w. $\mathcal{M}^f_\Phi, |w|_\Phi \models p$ für alle $p \in$ VAR.

(I.S.) Sei $\varphi = \neg\phi$. Nach Induktionsannahme gilt $\mathcal{M}, w \models \phi$ genau dann, wenn $\mathcal{M}^f_\Phi, |w|_\Phi \models \phi$, da Φ unter Teilformeln abgeschlossen ist und somit $\phi \in \Phi$ gilt. Wir haben also:

$$\begin{aligned} \mathcal{M}, w \models \neg\phi &\Leftrightarrow \mathcal{M}, w \not\models \phi \\ &\Leftrightarrow \mathcal{M}^f_\Phi, |w|_\Phi \not\models \phi \\ &\Leftrightarrow \mathcal{M}^f_\Phi, |w|_\Phi \models \neg\phi \end{aligned}$$

Analog gilt für $\varphi = \phi \wedge \psi$ nach Induktionsannahme $\mathcal{M}, w \models \phi$ g.d.w. $\mathcal{M}^f_\Phi, |w|_\Phi \models \phi$ und $\mathcal{M}, w \models \psi$ g.d.w. $\mathcal{M}^f_\Phi, |w|_\Phi \models \psi$. Es gilt also:

$$\begin{aligned} \mathcal{M}, w \models \phi \wedge \psi &\Leftrightarrow \mathcal{M}, w \models \phi \text{ und } \mathcal{M}, w \models \psi \\ &\Leftrightarrow \mathcal{M}^f_\Phi, |w|_\Phi \models \phi \text{ und } \mathcal{M}^f_\Phi, |w|_\Phi \models \psi \\ &\Leftrightarrow \mathcal{M}^f_\Phi, |w|_\Phi \models \phi \wedge \psi \end{aligned}$$

(I.S.) $\underline{n \mapsto n+1}$: Es gelte $\mathcal{M}^f_\Phi, |w|_\Phi \models \theta \Leftrightarrow \mathcal{M}, w \models \theta$ für alle θ mit $d(\theta) \leq n$.

Dann sei $\varphi = \Diamond\phi \in \Phi$.

„$\Rightarrow$“: Es gelte $\mathcal{M}, w \models \Diamond\phi$. Dann hat w in $\mathcal{M}$ eine Nachfolgerwelt v, sodass $\mathcal{M}, v \models \phi$. Es gilt dann $(w, v) \in R$ und nach (2) der Definition von $\mathcal{M}^f_\Phi$, dass $(|w|_\Phi, |v|_\Phi) \in R^f$. Nach Induktionsannahme gilt dann auch $\mathcal{M}^f_\Phi, |v|_\Phi \models \phi$, da $\phi \in \Phi$ wegen des Abschlusses von Φ unter Teilformeln ist.

Aus $(|w|_\Phi, |v|_\Phi) \in R^f$ und $\mathcal{M}^f_\Phi, |v|_\Phi \models \phi$ folgt $\mathcal{M}^f_\Phi, |w|_\Phi \models \Diamond\phi$.

„$\Leftarrow$“: Es gelte $\mathcal{M}^f_\Phi, |w|_\Phi \models \Diamond\phi$. Dann gibt es eine Welt $|v|_\Phi \in W^f$, sodass $\mathcal{M}^f_\Phi, |v|_\Phi \models \phi$ und $(|w|_\Phi, |v|_\Phi) \in R^f$. Da $\phi \in \Phi$ (s.o.), folgt nach Induktionsannahme, dass $\mathcal{M}, v \models \phi$. Schließlich folgt dann aber durch (3), dass $\mathcal{M}, w \models \Diamond\phi$.

□

Lemma 3.6. *Es sei $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ eine unter Teilformeln abgeschlossene Formelmenge und $\mathcal{M} = (W, R, V)$ ein Modell. Dann gilt $|W_\Phi| \leq 2^n$.*

Beweis. Sei $f\colon W_\Phi \to \mathcal{P}(\Phi)$ durch $|w|_\Phi \mapsto \{\varphi \in \Phi \mid \mathcal{M}, w \models \varphi\}$ definiert. Für zwei Welten $w, v \in W$ folgt aus $f(|v|_\Phi) = f(|w|_\Phi)$, dass in v und w genau die gleichen Formeln aus Φ erfüllt sind, also $v \sim_\Phi w$. Es folgt also weiter $|v|_\Phi = |w|_\Phi$, d.h. f ist injektiv. Daraus folgt aber mit Lemma 2.1 und 2.2 $|W_\Phi| \leq |\mathcal{P}(\Phi)| = 2^{|\Phi|} = 2^n$. □

Die entstehenden Äquivalenzklassen (ÄK) können auch explizit über die in ihren Welten geltenden Formeln aus Φ angegeben werden. Dadurch, dass im gegebenen Modell selten alle Kombinationen abgedeckt werden, ist die Anzahl der Äquivalenzklassen in der Regel deutlich kleiner als 2^n, etwa für den Fall, dass wie z.B. bei $\varphi_1 = \Diamond p, \varphi_2 = \neg\Diamond p$ die Formeln in $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ widersprüchlich sind.

ÄK	erfüllte Formeln			
0	$\neg\varphi_1$	...	$\neg\varphi_{n-1}$	$\neg\varphi_n$
1	$\neg\varphi_1$	...	$\neg\varphi_{n-1}$	φ_n
2	$\neg\varphi_1$	...	φ_{n-1}	$\neg\varphi_n$
...	...	...	...	...
$2^n - 1$	φ_1	...	φ_{n-1}	φ_n

Tabelle 3.1: Äquivalenzklassen der Relation $\sim_\Phi$ für $\Phi = \{\varphi_1, \ldots, \varphi_n\}$

Mithilfe dieser beiden Eigenschaften sind wir schließlich in der Lage, zu zeigen, dass die einfache Modallogik die endliche Modelleigenschaft besitzt.

Satz 3.7 (Endliche Modelleigenschaft der einfachen Modallogik)**.** *Es sei φ eine modallogische Formel. Falls es ein Modell gibt, das φ erfüllt, dann gibt es auch ein endliches Modell, das φ erfüllt.*

Beweis. Es sei $\mathcal{M} = (W, R, V)$ ein Modell, sodass $\mathcal{M}, w \models \varphi$ für ein $w \in W$. Setze $\Phi := \mathsf{sub}(\varphi)$, wobei $\mathsf{sub}(\varphi)$ die Menge der Teilformeln von φ bezeichnet. Insbesondere gilt $\varphi \in \mathsf{sub}(\varphi)$.

Konstruiere nun $\mathcal{M}^f_\Phi = (W^f, R^f, V^f)$. Offenbar ist $\mathsf{sub}(\varphi)$ endlich. Setze also $m := |\mathsf{sub}(\varphi)|$. Nach Lemma 3.6 gilt dann $|W_\Phi| \leq 2^m$, insbesondere ist W_Φ also endlich. Daraus folgt, dass auch $W^f = W_\Phi$ endlich ist. Insgesamt ist $\mathcal{M}^f_\Phi$ damit ein endliches Modell.

Nach Voraussetzung gilt $\mathcal{M}, w \models \varphi$. Nach Lemma 3.5 gilt somit auch $\mathcal{M}^f_\Phi, |w|_\Phi \models \varphi$, also ist $\mathcal{M}^f_\Phi$ ein endliches Modell, das φ erfüllt. □

3.1.2 Modallogisches Erfüllbarkeitsproblem

Besondere Auswirkungen hat dieses Resultat zum Beispiel auf Entscheidungsprobleme im Zusammenhang mit der Modallogik, sodass der Beweis der Entscheidbarkeit von ModalSAT direkt aus der endlichen Modelleigenschaft folgt. Für eine gegebene modallogische Formel φ kann nun eine obere Schranke für die Anzahl der minimal erforderlichen Welten in einem erfüllenden Modell angegeben werden. Die zu untersuchenden Modelle beschränken sich dadurch auf eine endliche Zahl, was einen einfachen (wenn auch ineffizienten) Entscheidungsalgorithmus liefert.

Korollar 3.8. ModalSAT *ist entscheidbar.*

Beweis. Es sei $\varphi \in \mathsf{FORM}_{\mathsf{ML}}$ Angenommen, φ ist erfüllbar. Dann gibt es ein Modell $\mathcal{M}$, das φ erfüllt. Dann erfüllt auch $\mathcal{M}^f_{\mathsf{sub}(\varphi)}$ die Formel φ, d.h. es gibt ein endliches Modell mit höchstens $n := 2^{|\mathsf{sub}(\varphi)|}$ Welten, das φ erfüllt. Es genügt also, für alle Modelle mit $\leq n$ Welten zu prüfen, ob sie φ erfüllen. Der folgende Algorithmus leistet das Gewünschte:

Eingabe: Modallogische Formel φ, die o.B.d.A. nur die Variablen $p_1, \ldots, p_k$ enthält.

$n := 2^{|\mathsf{sub}(\varphi)|}$
for all $1 \leq i \leq n$ **do**
    Setze $W := \{w_1, \ldots, w_i\}$.
    for all $R \subseteq R \times R$ **do**
        for all $V : \{p_1, \ldots, p_k\} \to \mathcal{P}(W)$ **do**
            Definiere $\mathcal{M} = (W, R, V)$.
            for all $w \in W$ **do**
                if $\mathcal{M}, w \models \varphi$ **then return** „erfüllbar“
return „unerfüllbar“

Es gibt $|\mathcal{P}(W \times W)| = 2^{|W \times W|} = 2^{|W|^2}$ mögliche Relationen auf W. Die Anzahl möglicher Funktionen V ist durch $|\mathcal{P}(W)|^k$ beschränkt, also ebenfalls endlich.

Eine Formel kann schließlich durch sukzessives Auswerten aller Teilformeln in endlicher Zeit ausgewertet werden.

Der Algorithmus arbeitet damit nur auf endlichen Strukturen und alle Schleifen werden endlich oft ausgeführt, sodass das Ausprobieren aller möglichen Modelle in endlicher Zeit erfolgen kann. Insbesondere sind alle Schritte berechenbar. □

3.2 Verallgemeinerungen

3.2.1 Multi-Modallogik

Um zu zeigen, dass die Filtrierung sich nicht nur für den Nachweis der endlichen Modelleigenschaft einfacher Modallogik eignet, nehmen wir nachfolgend eine kleine Anpassung an der Definition vor, sodass sich die gesamte Argumentation auch für die Multi-Modallogik durchführen lässt. In dieser neuen Variante der Filtrierung fordern wir dabei für jeden Konnektor dieselben Eigenschaften wie im eindimensionalen Fall.

Definition 3.9. *Es sei $\mathcal{M} = (W, R_1, \ldots, R_n, V)$ ein Modell für eine Multi-Modallogik und Φ eine unter Teilformeln abgeschlossene Formelmenge von multi-modallogischen Formeln.*

Ein Modell $\mathcal{M}^f_\Phi = (W^f, R^f_1, \ldots, R^f_n, V^f)$ heißt Filtrierung von $\mathcal{M}$ über Φ, falls

(1) $W^f = W_\Phi$

(2) $(|w|_\Phi, |v|_\Phi) \in R^f_i$ *für alle* $(w, v) \in R_i$, $1 \leq i \leq n$.

(3) Falls $(|w|_\Phi, |v|_\Phi) \in R^f_i$ *und* $\Diamond_i \phi \in \Phi$, *dann gilt* $\mathcal{M}, v \models \phi \Rightarrow \mathcal{M}, w \models \Diamond_i \phi$ *für alle* $1 \leq i \leq n$.

(4) Für jede in Φ vorkommende Variable p gilt $|w|_\Phi \in V^f(p)$ g.d.w. $\mathcal{M}, w \models p$.

Anschließend gelten dieselben Resultate wie auch schon für die einfache Modallogik. Dass endliche Mengen Φ zu endlichen Filtrierungen führen, funktioniert vollständig analog. Auch die endliche Modelleigenschaft folgt aus der Eigenschaft

$$\mathcal{M}, w \models \varphi \Leftrightarrow \mathcal{M}^f_\Phi, |w|_\Phi \models \varphi$$

für alle $\varphi \in \Phi$ genauso wie bei der einfachen Modallogik. Daher beschränken wir uns hier auf den Beweis der soeben genannten Eigenschaft.

Lemma 3.10. *Es sei $\mathcal{M} = (W, R_1, \ldots, R_n, V)$ ein multi-modallogisches Modell und Φ abgeschlossen unter Teilformeln mit $\varphi \in \Phi$. Dann gilt*

$$\mathcal{M}^f_\Phi, |w|_\Phi \models \varphi \Leftrightarrow \mathcal{M}, w \models \varphi.$$

Beweis. Analog zu Lemma 3.5 führen wir eine Induktion über $d(\varphi)$ durch.

(I.A.) $\underline{d(\varphi) = 0}$:

Wie im Beweis von Lemma 3.5.

(I.S.) $\underline{n \mapsto n+1}$: Es gelte $\mathcal{M}^f_\Phi, |w|_\Phi \models \theta \Leftrightarrow \mathcal{M}, w \models \theta$ für alle θ mit $d(\theta) \leq n$.

Dann sei $\varphi = \Diamond_k \phi$ für ein k mit $1 \leq k \leq n$ und $d(\phi) = n$.

„$\Rightarrow$“: Es gelte $\mathcal{M}, w \models \Diamond_k \phi$. Dann existiert ein $v \in W$ mit $(w, v) \in R_k$ und $\mathcal{M}, v \models \phi$. Es folgt mit (2) aus der Definition von $\mathcal{M}^f_\Phi$, dass $(|w|_\Phi, |v|_\Phi) \in R^f_k$. Nach Induktionsannahme gilt dann auch $\mathcal{M}^f_\Phi, |v|_\Phi \models \phi$, da $\phi \in \Phi$ wegen des Abschlusses unter Teilformeln gilt und $d(\phi) \leq n$.

Es folgt aus $(|w|_\Phi, |v|_\Phi) \in R^f_k$ und $\mathcal{M}^f_\Phi, |v|_\Phi \models \phi$, dass $\mathcal{M}^f_\Phi, |w|_\Phi \models \Diamond_k \phi$ gilt.

„$\Leftarrow$“: Es gelte $\mathcal{M}^f_\Phi, |w|_\Phi \models \Diamond_k \phi$. Dann gibt es eine Welt $|v|_\Phi \in W^f$, sodass $\mathcal{M}^f_\Phi, |v|_\Phi \models \phi$ und $(|w|_\Phi, |v|_\Phi) \in R^f_k$. Da $\phi \in \Phi$ (s.o.), folgt nach Induktionsannahme, dass $\mathcal{M}, v \models \phi$. Schließlich folgt dann aber durch (3), dass $\mathcal{M}, w \models \Diamond_k \phi$.

□

Satz 3.11 (Endliche Modelleigenschaft der Multi-Modallogik)**.** *Es sei φ eine multi-modallogische Formel. Falls es ein Modell gibt, das φ erfüllt, dann gibt es auch ein endliches Modell, das φ erfüllt.*

Beweis. Analog zur endlichen Modell-Eigenschaft bei einfacher modaler Logik folgt die Behauptung aus Lemma 3.10 und der Endlichkeit von W_Φ bei endlichem Φ. □

3.2.2 Rahmeneigenschaften

Bisher haben wir für die einfache Modallogik stets betrachtet, ob für eine Formel, die auf einem *beliebigen* Rahmen erfüllbar ist, ein *beliebiger endlicher* Rahmen existiert, auf dem die Formel erfüllbar ist. Wir wollen die Untersuchung eindimensionaler Konnektoren nun damit abschließen, zu untersuchen, welche Rahmeneigenschaften Filtrierungen im Allgemeinen beibehalten und welche nicht.

Informell können wir Rahmenklassen als eine Teilmenge aller Kripke-Rahmen auffassen, sodass die Graphen aller zur Teilmenge gehörenden Rahmen bestimmte strukturelle Eigenschaften (z.B. Transitivität) erfüllen. Möglich ist formal z.B. eine axiomatische Einführung wie in [4] (im Falle von transitiven Rahmen muss dann stets $\Box\varphi \to \Box\Box\varphi$ erfüllt sein). Die nachfolgend abgebildete Tabelle enthält eine Auswahl möglicher Rahmenklassen, von denen wir hier allerdings nur einen Teil abdecken werden.

Für eine Rahmenklasse A und ein Modell $\mathcal{M} = (\mathcal{F}, V)$ mit einem Rahmen $\mathcal{F} \in A$ schreiben wir auch $\mathcal{M} \in A$.

Rahmenklasse	Eigenschaft
K	alle Rahmen
T	reflexive Rahmen
K4	transitive Rahmen
B	symmetrische Rahmen
S4	transitive und reflexive Rahmen
S5	Äquivalenzrelationen

Tabelle 3.2: Einige Rahmenklassen für Kripke-Modelle

Es schließt sich für Rahmeneigenschaften, die von der Filtrierung nicht beibehalten werden, das Problem an, dass wir für die entsprechenden Rahmenklassen die endliche Modelleigenschaft nicht mehr wie bisher gesehen nachweisen können. Tatsächlich gibt es sogar Rahmenklassen, die die endliche Modelleigenschaft gar nicht besitzen.

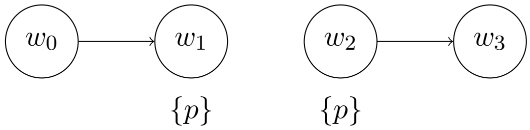
Zunächst schauen wir uns an, welche Eigenschaften die Filtrierung beibehält. Es ist offensichtlich, dass die Filtrierung die Reflexivität eines Modells beibehält, da für alle $\mathcal{M} = (W, R, V)$ mit $w \in W$ aus $(w, w) \in R$ stets $(|w|_\Phi, |w|_\Phi) \in R^f$ für alle Formelmengen Φ und Filtrierungen $\mathcal{M}_\Phi^f = (W^f, R^f, V^f)$ folgt.

Auch symmetrische Rahmen bleiben bei der Filtrierung erhalten, weil für $(|w|_\Phi, |v|_\Phi) \in R^f$ mit der Bemerkung auf Seite 16 folgt, dass es $w' \in |w|_\Phi, v' \in |v|_\Phi$ geben muss, sodass $(w', v') \in R$. Mit der Symmetrie von R folgt $(v', w') \in R$. Die Filtrierung ist dann wegen (2) aus Definition 3.3 auch symmetrisch.

Transitivität wird jedoch nicht beibehalten, wie das folgende Beispiel zeigt:

Beispiel 3.12

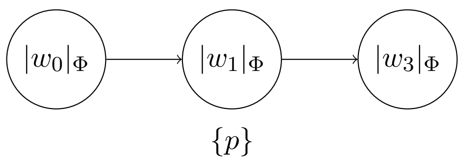
Wir betrachten das folgende Kripke-Modell $\mathcal{M} = (\mathcal{F}, V)$ mit $\mathcal{F}$ wie abgebildet und $V(p) = \{w_1, w_2\}$ sowie die Formelmenge $\Phi = \{p, \Diamond p\}$.



Offenbar ist der $\mathcal{M}$ zugrunde liegende Rahmen transitiv, allerdings lässt sich $\mathcal{M}_\Phi^f$ mithilfe der Äquivalenzklassen

- $|w_0|_\Phi$ mit $\mathcal{M}, w_0 \not\models p$ und $\mathcal{M}, w_0 \models \Diamond p$,
- $|w_1|_\Phi = |w_2|_\Phi$ mit der geltenden Formel p und
- $|w_3|_\Phi$ mit $\mathcal{M}, w_4 \not\models p$ und $\mathcal{M}, w_4 \not\models \Diamond p$

konstruieren wie folgt:



Nun ist $\mathcal{M}^f_\Phi$ aber nicht mehr transitiv, da $(|w_0|_\Phi, |w_1|_\Phi) \in R^f$ und $(|w_1|_\Phi, |w_3|_\Phi) \in R^f$, aber $(|w_0|_\Phi, |w_3|_\Phi) \notin R^f$.

Tatsächlich besitzt die einfache Modallogik, wenn man sie auf die Rahmenklasse $\mathsf{K4}$ einschränkt und zusätzlich Irreflexivität fordert, die endliche Modelleigenschaft *nicht*.

Satz 3.13. *Für die modale Basis* ML *der einfachen modalen Logik gilt:*

1. ML *besitzt die endliche Modelleigenschaft bzgl. der Rahmenklassen* T *und* B.
2. ML *besitzt* nicht *die endliche Modelleigenschaft bzgl. der Rahmenklasse aller transitiven, irreflexiven Rahmen*

Beweis. (1) folgt direkt daraus, dass die Filtrierung die entsprechenden Rahmeneigenschaften beibehält.

Für den Beweis von (2) konstruieren wir ein Gegenbeispiel mithilfe der Formel $\varphi := \Diamond p \wedge \Box\Diamond p$. Für $\mathcal{M} = (\mathbb{N}, <, V)$ und $V(p) = \mathbb{N}$ gilt $\mathcal{M}, 1 \models \varphi$, d.h. φ ist auf einem transitiven, irreflexiven Modell erfüllbar.

Gleichzeitig sei nun $\mathcal{M}' = (W', R', V')$ ein beliebiges transitives und irreflexives Modell, $w_0 \in W'$ und $\mathcal{M}', w_0 \models \varphi$. Wir zeigen nun durch Induktion, dass $\mathcal{M}$ einen unendlich langen Pfad der Form $w_0, w_1, w_2, \ldots$ mit $w_i \neq w_j$ für alle $i \neq j$ enthalten muss.

(I.A.) Da $\mathcal{M}, w_0 \models \Diamond p$ gelten muss und $\mathcal{M}$ irreflexiv ist, muss es eine Welt $w_1 \in W'$ mit $w_0 \neq w_1$ und $(w_0, w_1) \in R'$ und $w_1 \in V'(p)$ geben.

(I.S.) Es sei $w_0, \ldots, w_n \in W'$ mit $(w_i, w_{i+1}) \in R'$ für alle $0 \leq i < n$. Dann gilt wegen der Transitivität von R' auch $(w_0, w_n) \in R'$. Wegen $\mathcal{M}', w_0 \models \Box\Diamond p$ muss dann $\mathcal{M}', w_n \models \Diamond p$ gelten. Es muss also eine Welt $w' \in W'$ existieren mit $(w_n, w') \in R'$ und $w' \in V'(p)$. Zusätzlich gilt $w' \neq w_i$, da ansonsten die Kanten (w_i, w') und (w', w_i) in R' enthalten sein müssen und das Modell dann nicht mehr irreflexiv wäre.

Folglich impliziert die Gültigkeit von φ in einer Welt eines Modells die Existenz eines unendlichen einfachen Pfades. Wenn $\mathcal{M}'$ nun aber einen unendlich langen Pfad enthalten muss, ist $\mathcal{M}'$ selbst unendlich und φ damit nicht auf einem endlichen Modell erfüllbar. □

Es scheint etwas willkürlich, sich auf transitive, irreflexive Rahmen einzuschränken, doch diese Einschränkung haben wir bereits im zweiten Kapitel bei der Einführung der einfachen temporalen Logik gesehen. Außerdem wird im vierten Kapitel im Zusammenhang mit LTL ein vergleichbares Argument herangezogen.

Korollar 3.14. *Die einfache temporale Logik besitzt die endliche Modelleigenschaft nicht.*

Beweis. In der einfachen temporalen Logik sind nur transitive, irreflexive Rahmen zugelassen. □

3.3 Mehrdimensionale Konnektoren

Um das Kapitel über die modale Logik abzuschließen, lassen wir in diesem Abschnitt nun auch mehrdimensionale Konnektoren zu. Das präsentierte Vorgehen ist für den Fall unärer Konnektoren eine Alternative zur Filtrierung, allerdings mit dem großen Nachteil, dass deutlich weniger strukturerhaltende Eigenschaften existieren.

Die Idee für die hier präsentierte Argumentation ist schon aus dem zweiten Kapitel bekannt und basiert darauf, dass Formeln weder unendlich viele verschiedene Aussagen bis zu einer festen maximalen modalen Tiefe ausdrücken können noch unendlich weit blicken können (d.h. nur Welten, die durch entsprechend kurze Pfade erreichbar sind, sind überhaupt sichtbar – vgl. Beispiel 2.20). Bisher haben wir noch keine der beiden Behauptungen formal gezeigt. Wir beginnen daher damit, die erste Behauptung im folgenden Lemma zu beweisen.

Lemma 3.15. *Sei τ eine endliche modale Basis. Dann ist die Anzahl der (bis auf logische Äquivalenz) verschiedenen Formeln $\varphi \in \mathsf{FORM}_\tau$ über einer endlichen Variablenmenge mit $d(\varphi) \leq n$ für jedes $n \in \mathbb{N}$ endlich.*

Beweis. Wir führen eine Induktion über n durch.

(I.A.) Sei $\varphi \in \mathsf{FORM}_\tau$ mit $d(\varphi) = 0$. Ob φ in einer Welt w erfüllt ist, hängt nun ausschließlich von den in der Welt geltenden Variablen ab. Sei nun $|\mathsf{VAR}| = k$. Dann gibt es genau 2^{2^k} Möglichkeiten (für jede der 2^k Belegungen kann die Formel entweder wahr oder falsch sein), die in w geltenden Variablen auf einen Wahrheitswert abzubilden, also (bis auf Äquivalenz) nur endlich viele τ-Formeln von modaler Tiefe 0.

(I.S.) Die Aussage gelte für $1, \ldots, n$. Sei also $\Psi_n := \{\psi_1, \ldots, \psi_k\}$ so gewählt, dass für alle $\psi \in \mathsf{FORM}_\tau$ mit $d(\psi) \leq n$ gilt: $\psi \Leftrightarrow \psi_i$ für ein $\psi_i \in \Psi_n$. Ψ_n existiert nach Induktionsvoraussetzung. Für alle $\triangle \in O$ definiere

$$\Phi_n^{\triangle} := \{\triangle(\phi_1, \ldots, \phi_{\rho(\triangle)}) \mid \phi_i \in \Psi_n \text{ und } d(\phi_i) \leq n \text{ für alle } 1 \leq i \leq \rho(\triangle)\}$$

Da es für alle ϕ_i nur endlich viele Möglichkeiten gibt, gibt es entsprechend auch nur endlich viele Kombinationsmöglichkeiten, sodass $\Phi_n^{\triangle}$ endlich ist. Nun ist zudem $\Phi_n := \{\Phi_n^{\triangle} \mid \triangle \in O\}$ wegen der Endlichkeit von O eine endliche Vereinigung endlicher Mengen und damit selbst endlich.

Wenn wir nun Φ_n als Variablenmenge für Formeln mit modaler Tiefe $n+1$ auffassen, erhalten wir genau den Fall aus dem Induktionsanfang. Folglich ist auch $\{\varphi \in \mathsf{FORM}_\tau \mid d(\varphi) \leq n+1\}$ endlich.

□

Um die zweite Behauptung zu zeigen, benutzen wir n-Bisimulationen. Bisimulationen im Allgemeinen sind Relationen zwischen den Welten zweier Modelle, sodass immer genau solche Welten in Relation zueinander stehen, für die die gleichen Variablen gelten und von denen aus vergleichbare Welten erreichbar sind.

Der hier betrachtete Sonderfall schränkt die Forderung so ein, dass wir die erreichten Welten nur bis zu einer maximalen Pfadlänge überprüfen. Weil die Formeln ohnehin nur endlich weit blicken können, ist die Intuition, dass das ausreicht.

Definition 3.16 (n-Bisimulation)**.** *Es seien $n \in \mathbb{N}$, $\tau = (O, \rho)$ eine endliche modale Basis,* VAR *eine endliche Variablenmenge und $\mathcal{M} = (W, \{R_\triangle \mid \triangle \in O\}, V)$ sowie $\mathcal{M}' = (W', \{R'_\triangle \mid \triangle \in O\}, V')$ τ-Modelle mit $x \in \mathcal{M}, x' \in \mathcal{M}'$. Für eine Folge von Relationen $Z_n \subseteq Z_{n-1} \subseteq \cdots \subseteq Z_0 \subseteq W \times W'$ heißt Z_n eine n-Bisimulation zwischen x und x', falls*

(1) $(x, x') \in Z_n$

(2) $(w, w') \in Z_0 \Rightarrow V(w) = V'(w')$

(3) Für alle $0 \leq i < n$ und $\triangle \in O$: Falls $(w, w') \in Z_{i+1}$ und $(w, v_1, \ldots, v_{\rho(\triangle)}) \in R_\triangle$, dann existieren v'_j mit $(v_j, v'_j) \in Z_i$ und $(w', v'_1, \ldots, v'_{\rho(\triangle)}) \in R'_\triangle$ für alle $1 \leq j \leq \rho(\triangle)$.

(4) Für alle $0 \leq i < n$ und $\triangle \in O$: Falls $(w, w') \in Z_{i+1}$ und $(w', v'_1, \ldots, v'_{\rho(\triangle)}) \in R'_\triangle$, dann existieren v_j mit $(v_j, v'_j) \in Z_i$ und $(w, v_1, \ldots, v_{\rho(\triangle)}) \in R_\triangle$ für alle $1 \leq j \leq \rho(\triangle)$.

Falls zwischen x und x' eine n-Bisimulation existiert, schreiben wir auch $x \rightleftarrows_n x'$.

Die strukturerhaltende Eigenschaft von n-Bismulationen, die wir intuitiv auch herbeiführen wollten, ist, dass in zwei Welten w, w' in zwei Modellen $\mathcal{M}, \mathcal{M}'$ mit $w \rightleftarrows_n w'$ die gleichen modallogischen Formeln mit modaler Tiefe $\leq n$ erfüllt sind.

Lemma 3.17. *Sei τ eine endliche modale Basis,* VAR *eine endliche Variablenmenge und $\mathcal{M}, \mathcal{M}'$ τ-Modelle. Dann sind für alle Welten w aus $\mathcal{M}$ und w' aus $\mathcal{M}'$ die folgenden Aussagen äquivalent:*

(1) $w \rightleftarrows_n w'$

(2) Für alle $\varphi \in \mathsf{FORM}_\tau$ mit $d(\varphi) \leq n$ gilt $\mathcal{M}, w \models \varphi \Leftrightarrow \mathcal{M}', w' \models \varphi$.

Beweis. „$\Rightarrow$“: Wir führen eine Induktion über n durch.

(I.A.) Falls $w \rightleftarrows_0 w'$, dann gilt nach Definition $V(w) = V(w')$. Da alle modallogischen Formeln mit der modalen Tiefe 0 aussschließlich von den in der Welt, in der sie ausgewertet werden, geltenden Variablen abhängen, folgt daraus die Behauptung.

(I.S.) Es gelte (1) $\Rightarrow$ (2) für alle $m \leq n$.

Sei $\triangle \in O$ beliebig und $\rho(\triangle) = k$. Dann seien $\phi_1, \ldots, \phi_k \in \mathsf{FORM}_\tau$ mit $d(\phi_i) \leq n$ für alle $1 \leq i \leq k$ und $w \rightleftarrows_{n+1} w'$.

$$
\begin{aligned}
&\mathcal{M}, w \models \triangle(\phi_1, \ldots, \phi_k) \\
\Leftrightarrow\ & \exists\, v_1, \ldots, v_k \in W \text{ mit } (w, v_1, \ldots, v_k) \in R_\triangle, \mathcal{M}, v_i \models \phi_i\ \forall i : 1 \leq i \leq k \\
\Rightarrow\ & \exists\, v'_1, \ldots, v'_k \in W' \text{ mit } (w', v'_1, \ldots, v'_k) \in R'_\triangle, v_i \rightleftarrows_n v'_i\ \forall i : 1 \leq i \leq k \\
\Rightarrow\ & \exists\, v'_1, \ldots, v'_k \in W' \text{ mit } (w', v'_1, \ldots, v'_k) \in R'_\triangle, \mathcal{M}', v'_i \models \phi_i\ \forall i : 1 \leq i \leq k \\
\Leftrightarrow\ & \mathcal{M}', w' \models \triangle(\phi_1, \ldots, \phi_k)
\end{aligned}
$$

Die dritte Zeile folgt mit $w \rightleftarrows_{n+1} w'$ aus Bedingung (2) der Definition 3.16 und die vierte Zeile aus der Induktionsvoraussetzung mit $d(\phi_i) \leq n$ für alle i. Die Rückrichtung von $\mathcal{M}'$ nach $\mathcal{M}$ kann exakt analog gezeigt werden.

„$\Leftarrow$“: Sei $\mathcal{M} = (W, R, V)$ und $\mathcal{M}' = (W', R', V')$. Wir zeigen, dass

$$Z_k = \{(v, v') \in W \times W' | \mathcal{M}, v \models \varphi \Leftrightarrow \mathcal{M}', v' \models \varphi \text{ für alle } \varphi \in \mathsf{FORM}_\tau \text{ mit } d(\varphi) \leq k\}$$

mit $0 \leq k \leq n$ eine n-Bisimulation ist. Für $w \in W$ und $w' \in W'$ gelte dafür (2). Es lässt sich nun nachprüfen, dass dann (1) bis (4) aus Definition 3.16 erfüllt sind.

(1) und (2) gelten offensichtlich nach Voraussetzung. Wähle $(w, w') \in Z_k$ für ein $1 \leq k \leq n$. Wir nehmen nun an, dass ein $v \in W$ existiert, das Bedingung (3) verletzt, d.h. für ein $\triangle \in O$ gibt es eine Kante $(w, v_1, \dots, v_{\rho(\triangle)}) \in R_\triangle$, für die keine $v'_1, \dots, v'_{\rho(\triangle)} \in W'$ existieren mit $(w', v'_1, \dots, v'_{\rho(\triangle)}) \in R'_\triangle$ und $(v_i, v'_i) \in Z_{k-1}$ für alle $1 \leq i \leq \rho(\triangle)$.

Sei also $S' = \{(v'_1, \dots, v'_{\rho(\triangle)}) \in W' \times \cdots \times W' \mid (w', v'_1, \dots, v'_{\rho(\triangle)}) \in R'_\triangle\}$ die Menge aller Nachfolgertupel von w' in $\mathcal{M}'$. S' ist nichtleer, da ansonsten $\mathcal{M}', w' \models \neg\triangle(\top, \dots, \top)$, aber $\mathcal{M}, w \models \triangle(\top, \dots, \top)$, weil w Nachfolger $v_1, \dots, v_{\rho(\triangle)}$ hat (und dann wäre $(w, w') \notin Z_k$).

Nun muss es für alle $(v'_1, \dots, v'_{\rho(\triangle)}) \in S'$ ein $1 \leq i \leq \rho(\triangle)$ und eine Formel ϕ mit $d(\phi) \leq k - 1$ geben, sodass $\mathcal{M}', v'_i \not\models \phi$, aber $\mathcal{M}, v_i \models \phi$. Setze für jedes solche ϕ $f(\phi) = i$. Da nach Lemma 3.15 nur endlich viele logisch nicht äquivalente Formeln mit modaler Tiefe $\leq k - 1$ existieren, lässt sich eine endliche Liste solcher Formeln $\phi_1, \dots, \phi_n$ finden, sodass für alle $(v'_1, \dots, v'_{\rho(\triangle)})$ wie oben ein i existiert mit $\mathcal{M}', v'_i \not\models \phi_j$ und $\mathcal{M}, v_i \models \phi_j$ für ein ϕ_j mit $f(\phi_j) = i$. Es folgt dann aber für

$$\varphi := \triangle\Big(\bigwedge_{\{j \mid f(\phi_j)=1\}} \phi_j, \bigwedge_{\{j \mid f(\phi_j)=2\}} \phi_j, \dots, \bigwedge_{\{j \mid f(\phi_j)=\rho(\triangle)\}} \phi_j\Big),$$

dass $\mathcal{M}, w \models \varphi$ und $\mathcal{M}', w' \not\models \varphi$. Weil für alle ϕ_j gilt: $d(\phi_j) \leq k - 1$, muss $d(\varphi) \leq k$ gelten. Dann folgt aber $(w, w') \notin Z_k$ im Widerspruch zur Annahme. Damit muss (3) aus der Definition der Bisimulation erfüllt sein. (4) folgt analog. $\square$

Definition 3.18. *Sei $\tau = (O, \rho)$ und $\mathcal{M} = (W, \{R_\triangle \mid \triangle \in O\}, V)$ ein τ-Modell. Falls es einen Konnektor $\triangle$ mit Stelligkeit n und eine Kante $(w, v_1, \dots, v_n) \in R_\triangle$ gibt, nennen wir $v_1, \dots, v_n$ die Nachfolger von w und schreiben $\mathsf{suc}(w, v_i)$ für alle $1 \leq i \leq n$.*

Falls $\mathcal{M}$ die Eigenschaft besitzt, dass ein $w \in W$ existiert, sodass

- *zu jeder Welt $v \in W$ mit $w \neq v$ ein eindeutiger Pfad von w nach v (d.h. eine Folge $w = v_0, v_1, \dots, v_k = v$, sodass $\mathsf{suc}(v_i, v_{i+1})$ für alle $0 \leq i < n$) existiert und*
- *keine Zyklen, also Folgen $v_1, \dots, v_k = v_1$ mit $\mathsf{suc}(v_i, v_{i+1})$ für alle $0 \leq i < k$, existieren,*

heißt $\mathcal{M}$ verwurzelt *in w bzw.* baumartig. *In diesem Fall heißt w die* Wurzel *von $\mathcal{M}$.*

Für alle Welten in $w \in W$ definieren wir deren Höhe *$h(w)$ wie folgt:*

- *$h(w) = 0$ für die Wurzel von $\mathcal{M}$.*
- *Für alle Welten w mit Höhe n und alle v mit $\mathsf{suc}(w, v)$ setze $h(v) := n + 1$, falls v keine kleinere Höhe als $n + 1$ zugewiesen wurde.*

Die Höhe eines Modells ist $\max\{h(v) \mid v \in W\}$.

Für $k \in \mathbb{N}$ definieren wir $(\mathcal{M} \restriction k) := (W^k, \{R^k_\triangle \mid \triangle \in O\}, V^k)$, wobei $W^k := \{w \in W \mid h(w) \leq k\}$, $R^k_\triangle := W^k \times \cdots \times W^k \cap R_\triangle$ für alle $\triangle \in O$ und $V^k(p) = V(p) \cap W^k$ für alle $p \in \mathsf{VAR}$.

Als Nächstes nutzen wir die in Lemma 3.17 gezeigte Eigenschaft aus, um Welten zu eliminieren, die für eine Formel nicht sichtbar sind. Wir transformieren die Modelle dafür zu baumartigen Modellen und schneiden alle Pfade bei entsprechender Entfernung zur Wurzel (in der wir unsere Formel auswerten) ab. Lemma 3.19 und 3.20 weisen formal nach, dass wir diese beiden Operationen so durchführen können, dass unsere Formel dabei auf jeden Fall erfüllt bleibt.

Lemma 3.19. *Sei $\tau = (O, \rho)$ eine modale Basis. Jede erfüllbare Formel $\varphi \in \mathsf{FORM}_\tau$ ist auf einem baumartigen Modell erfüllbar.*

Beweis. Sei $\mathcal{M} = (W, \{R_\triangle \mid \triangle \in O\}, V)$ ein Modell, sodass $\mathcal{M}, w \models \varphi$ für ein $w \in W$. Wir konstruieren $\mathcal{M}' = (W', \{R'_\triangle \mid \triangle \in O\}, V')$, indem wir W' minimal wählen, sodass für alle $\triangle \in O$ und $R'_\triangle = R_\triangle \cap W' \times \cdots \times W'$ gilt:

- Falls $w \in W'$ und $(w, v_1, \ldots, v_{\rho(\triangle)}) \in R_\triangle$, dann gilt auch $v_1, \ldots, v_{\rho(\triangle)} \in W'$

Wir setzen $V'(w) = V(w) \cap W'$ für alle $w \in W'$.

Behauptung 1: $\mathcal{M}', w \models \varphi$.

Beweis. Wir führen eine Induktion über φ durch, bei der wir die rekursive Definition von FORM_τ ausnutzen, um zu zeigen, dass $\mathcal{M}, w \models \varphi \Leftrightarrow \mathcal{M}', w \models \varphi$ für alle $\varphi \in \mathsf{FORM}_\tau$ und $w \in W'$.

(I.A.) Für alle Variablen p gilt $w \in V(p) \Leftrightarrow w \in V'(p)$ für alle $w \in W'$. Folglich gilt $\mathcal{M}, w \models p \Leftrightarrow w \in V(p) \Leftrightarrow w \in V'(p) \Leftrightarrow \mathcal{M}', w \models p$.

(I.S.) Es gelte die Aussage für $\phi, \psi \in \mathsf{FORM}_\tau$ und es sei $w \in W'$.

- $\mathcal{M}, w \models \neg\phi \Leftrightarrow \mathcal{M}, w \not\models \phi \Leftrightarrow \mathcal{M}', w \not\models \phi \Leftrightarrow \mathcal{M}', w \models \neg\phi$. Die erste und dritte Äquivalenz folgt aus der Definition der Erfülltheit von Formeln, die zweite aus der Induktionsvoraussetzung.
- $\mathcal{M}, w \models \phi \wedge \psi \Leftrightarrow \mathcal{M}, w \models \phi$ und $\mathcal{M}, w \models \psi \Leftrightarrow \mathcal{M}', w \models \phi$ und $\mathcal{M}', w \models \psi \Leftrightarrow \mathcal{M}', w \models \phi \wedge \psi$.
- Sei $\triangle \in \rho$ mit $\rho(\triangle) = k$. Dann gelte die Aussage für $\phi_1, \ldots, \phi_k \in \mathsf{FORM}_\tau$. Es folgt $\mathcal{M}', w \models \triangle(\phi_1, \ldots, \phi_k) \Leftrightarrow$ es existiert eine Kante $(w, v_1, \ldots, v_k) \in R_\triangle$, sodass $\mathcal{M}, v_i \models \phi_i$ für alle $1 \leq i \leq k$. Weil $w \in W'$, müssen nach Konstruktion von W' auch $v_1, \ldots, v_k \in W'$ und $(w, v_1, \ldots, v_k) \in R'_\triangle$ sein und nach Induktionsvoraussetzung gilt $\mathcal{M}', v_i \models \phi$. Das ist äquivalent zu $\mathcal{M}', w \models \triangle(\phi_1, \ldots, \phi_k)$. Die Gegenrichtung gilt analog.

Behauptung 1 □

Schließlich definieren wir $\mathcal{M}_T = (W_T, \{R_{\triangle,T} \mid \triangle \in O\}, V_T)$ folgendermaßen:

- W_T besteht aus allen endlichen Folgen $(v_0, v_1, \ldots, v_m)$ von Welten aus W', für die $v_0 = w$ und $\mathsf{suc}(v_i, v_{i+1})$ für alle $0 \leq i < m$ gilt.
- Für $v_i = (v_{i,1}, v_{i,2}, \ldots, v_{i,a_i}) \in W_T$ gilt $(v_0, v_1, \ldots, v_{\rho(\triangle)}) \in R_{\triangle,T}$ genau dann, wenn $a_1 = a_2 = \cdots = a_{\rho(\triangle)} = a_0 + 1$ und $(v_{0,a_0}, v_{1,a_1}, \ldots, v_{\rho(\triangle),a_{\rho(\triangle)}}) \in R'_\triangle$.
- Für alle Variablen p setze $V_T(p) = \{(v_0, \ldots, v_k) \in W_T \mid v_k \in V'(p)\}$.

Behauptung 2: Für alle $n \in \mathbb{N}$ gilt: $\mathcal{M}, w \rightleftarrows_n \mathcal{M}_T, (w)$

Beweis. Definiere dafür $Z = \{(v, (v_0, \dots, v_k)) \in W' \times W_T \,|\, v = v_k\}$. Setzt man $Z_n = Z$ für alle n, erhält man die gewünschte n-Bisimulation. Wir prüfen nun die Voraussetzungen aus 3.16:

(2) Nach Konstruktion von V_T gilt $v \in V'(p)$ g.d.w. $(v_0, \dots, v_k) \in V_T(p)$.

(3) Sei $w \in W'$ und $v = (v_0, \dots, v_k) \in W_T$, sodass $(w, v) \in Z$. Für ein $\triangle \in O$ gelte zudem $(w, w_1, \dots, w_{\rho(\triangle)}) \in R'_\triangle$. Dann gibt es auch Folgen $a_j = (v_0, \dots, v_k, w_j) \in W_T$ für alle $1 \leq j \leq \rho(\triangle)$ und nach Definition von Z ist $(w_j, a_j) \in Z$. Schließlich ist $R_{\triangle,T}$ so definiert, dass nun auch $(v, a_1, \dots, a_{\rho(\triangle)}) \in R_{\triangle,T}$ gilt.

(4) Sei $w \in W'$ und $v = (v_0, \dots, v_k) \in W_T$, sodass $(w, v) \in Z$. Für ein $\triangle \in O$ gelte zudem $(v, v_1, \dots, v_{\rho(\triangle)}) \in R_{\triangle,T}$. Dann muss für alle $1 \leq j \leq \rho(\triangle)$ $v_j = (v_0, \dots, v_k, w_j)$ für ein $w_j \in W'$ sein. Wiederum nach Definition von $R_{\triangle,T}$ muss auch $(v_k, w_1, \dots, w_{\rho(\triangle)}) \in R_{\triangle,T}$ gelten. Außerdem gilt natürlich $(w_j, (v_0, \dots, v_k, w_j)) \in Z$ für alle j.

Die Folge $Z_n \subseteq Z_{n-1} \subseteq \cdots \subseteq Z_0$ mit $Z_i = Z$ für alle $0 \leq i \leq n$ erfüllt also alle Voraussetzungen für eine n-Bisimulation. Behauptung 2 □

Sei nun $d(\varphi) = k$. Dann gilt insbesondere $\mathcal{M}, w \rightleftarrows_k \mathcal{M}_T, (w)$ und damit $\mathcal{M}, w \models \varphi \Leftrightarrow \mathcal{M}_T, (w) \models \varphi$ (Lemma 3.17). $\mathcal{M}_T$ ist nach Konstruktion azyklisch und damit baumartig mit Wurzel (w) (die in 3.18 geforderten Pfade existieren nach Konstruktion von $\mathcal{M}'$), sodass insgesamt folgt, dass φ auf einem baumartigen Modell erfüllbar ist. □

Lemma 3.20. *Sei $\tau = (O, \rho)$ eine modale Basis und $\mathcal{M}$ ein τ-Modell, das in einer Welt w verwurzelt ist. Dann gilt für jede Welt in $(\mathcal{M} \upharpoonright k)$: $(\mathcal{M} \upharpoonright k), w \rightleftarrows_n \mathcal{M}, w$ für $n = k - h(w)$.*

Beweis. Sei k beliebig und w eine Welt aus $\mathcal{M} = (W, \{R_\triangle | \triangle \in O\}, V)$ mit $h(w) \leq k$. Wir zeigen mit Induktion über i: Für $Z_i := \{(w, w) \in W \times W^k \mid h(w) \leq k - i\}$ ist $Z_i \subseteq \cdots \subseteq Z_0$ eine i-Bisimulation für alle $0 \leq i \leq k$.

(I.A.) Für alle $w \in W^k$ gelten nach Konstruktion von $(\mathcal{M} \upharpoonright k)$ die gleichen Variablen wie in der gleichnamigen Welt in W. Damit erfüllt Z_0 die Voraussetzungen.

(I.S.) Sei $m < k$. Wir nehmen an, dass Z_i für alle $0 \leq i \leq m$ die Voraussetzungen erfüllt.

Wir zeigen nun, dass für alle $(v, v) \in Z_{m+1}$ die Voraussetzungen erfüllt sind. Sei dafür $(v, v_1, v_2, \dots, v_{\rho(\triangle)}) \in R_\triangle$ für ein $\triangle \in O$. Da $h(v) < k - m$ (nach Konstruktion von Z_{m+1}), muss für alle v_i ($1 \leq i \leq \rho(\triangle)$) gelten: $h(v_i) \leq k - m$, d.h. alle v_i sind auch Welten in $(\mathcal{M} \upharpoonright k)$. Es muss also auch $(v, v_1, v_2, \dots, v_{\rho(\triangle)}) \in R^k_\triangle$ gelten. Ebenfalls gilt dann $(v_i, v_i) \in Z_m$. Damit gilt (3) aus der Definition der Bisimulation. Die Gültigkeit von (4) folgt analog.

Damit haben wir insgesamt gezeigt, dass alle Z_i die Voraussetzungen für eine i-Bisimulation erfüllen. Sei nun $n = k - h(w)$. Dann gilt $(w, w) \in Z_n$, woraus direkt die Aussage $(\mathcal{M} \upharpoonright k), w \rightleftarrows_n \mathcal{M}, w$ folgt. □

Schließlich können wir die beiden letzten Ergebnisse nutzen, um ein gegebenes Modell zunächst zu einem Baum endlicher Höhe zu vereinfachen und anschließend in einem weiteren Schritt aus den Nachfolgern der übrigen Knoten jeweils endlich viele auswählen, um ein endliches Modell zu erhalten. Daraus folgt anschließend die endliche Modelleigenschaft.

Satz 3.21 (Endliche Modelleigenschaft für mehrdimensionale Konnektoren)**.** *Sei $\tau = (O, \rho)$ eine modale Basis. Dann kann jede erfüllbare τ-Formel auch auf einem endlichen Modell erfüllt werden.*

Beweis. Sei $\varphi \in \mathsf{FORM}_\tau$ und $d(\varphi) = k$. Wir definieren VAR als die Menge der in φ vorkommenden Variablen und $\tau' = (O', \rho')$, sodass O' nur die in φ vorkommenden modalen Konnektoren enthält und $\rho'(\triangle) = \rho(\triangle)$ für alle $\triangle \in O'$.

Sei nun $\mathcal{M}_1, w_1$ so gewählt, dass $\mathcal{M}_1, w_1 \models \varphi$. Mit Lemma 3.19 folgt, dass ein in w_2 verwurzeltes Modell $\mathcal{M}_2$ existiert, sodass $\mathcal{M}_2, w_2 \models \varphi$. Wir definieren nun $\mathcal{M}_3 = (W, \{R_\triangle | \triangle \in O'\}, V) := (\mathcal{M}_2 \upharpoonright k)$. Mit Lemma 3.20 folgt $\mathcal{M}_2, w_2 \rightleftarrows_k \mathcal{M}_3, w_2$ und wegen $d(\varphi) = k$ folgt mit Lemma 3.17, dass $\mathcal{M}_3, w_2 \models \varphi$.

Da es Welten in $\mathcal{M}_3$ mit unendlich vielen Nachfolgern geben kann, wählen wir im nächsten Schritt jeweils endlich viele dieser Nachfolger aus, um ein endliches Modell $\mathcal{M}_4$ zu erhalten.

Sei dazu $W_0 = \{w_2\}$. Wir definieren nun W_{n+1} induktiv: Sei $w \in W_n$. Dann können alle nicht-äquivalenten Formeln mit modaler Tiefe $\leq k - n$ nach Lemma 3.15 in einer endlichen Liste $\phi_1, \ldots, \phi_m$ aufgeschrieben werden.

Für alle $1 \leq i \leq m$: Falls $\mathcal{M}_3, w \models \phi_i$ und ϕ_i der Form $\triangle(\psi_1, \ldots, \psi_{\rho(\triangle)})$ für ein $\triangle \in O'$ ist, dann existiert eine Kante $(w, v_1, \ldots, v_{\rho(\triangle)}) \in R_\triangle$ mit $\mathcal{M}_3, v_j \models \psi_j$ für alle $1 \leq j \leq \rho(\triangle)$. Setze $W^i_{n+1}(w) := \{v_1, \ldots, v_{\rho(\triangle)}\}$ für eine beliebige solche Kante.

Wir setzen nun

$$W_{n+1}(w) := \bigcup_{1 \leq i \leq m} W^i_{n+1}(w) \text{ und } W_{n+1} := \bigcup_{w \in W_n} W_{n+1}(w).$$

Schließlich definieren wir $\mathcal{M}_4 = (W', \{R'_\triangle \mid \triangle \in O'\}, V')$ mit den Welten $W' := W_0 \cup \cdots \cup W_k$, indem wir die Relationen und die Auswertungsfunktion für Variablen aus $\mathcal{M}_3$ auf W' einschränken. W' ist endlich, da alle $W_i, 1 \leq i \leq k$ endlich sind.

Wir können außerdem mit Induktion zeigen, dass für alle $\phi \in \mathsf{FORM}_\tau$ mit $d(\phi) \leq n$ gilt: $\mathcal{M}_4, w \models \phi \Leftrightarrow \mathcal{M}_3, w \models \phi$ für alle $w \in W'$ mit $h(w) \leq k - n$.

(I.A.) Da die Auswertungsfunktion von $\mathcal{M}_4$ der aus $\mathcal{M}_3$ entspricht, ist die Aussage für alle ϕ mit $d(\phi) = 0$ trivial wahr.

(I.S.) Es gelte nun $\mathcal{M}_3, w \models \phi \Leftrightarrow \mathcal{M}_4, w \models \phi$ für alle $\phi \in \mathsf{FORM}_\tau, w \in W'$ mit $d(\phi) \leq n$ und $h(w) \leq k - n$.

Wir wählen eine Welt $v \in W'$ mit $h(v) \leq k - n - 1$. Sei $\triangle \in O'$, $\rho(\triangle) = k$ und ϕ der Form $\triangle(\phi_1, \ldots, \phi_k)$ für $d(\phi_i) \leq n$ für $i = 1, \ldots, k$.

„$\Rightarrow$“: Es gelte $\mathcal{M}_3, w \models \phi$. Dann gibt es $v_1, \ldots, v_k \in W$, sodass $\mathcal{M}_3, v_i \models \phi_i$ für alle $1 \leq i \leq k$ und $(w, v_1, \ldots, v_k) \in R_\triangle$. Nun muss es nach Konstruktion von W' auch Welten $v'_1, \ldots, v'_k \in W'$ geben mit $(w, v'_1, \ldots, v'_k) \in R'_\triangle$ und $\mathcal{M}_3, v'_i \models \phi_i$, also nach Induktionsvoraussetzung auch $\mathcal{M}_4, v'_i \models \phi_i$. Es gilt folglich $\mathcal{M}_4, w \models \phi$.

„$\Leftarrow$“: Umgekehrt gelte nun $\mathcal{M}_4, w \models \phi$. Dann gibt es $v_1, \ldots, v_k \in W'$, sodass $\mathcal{M}_4, v_i \models \phi_i$ für alle $1 \leq i \leq k$ und $(w, v_1, \ldots, v_k) \in R'_\triangle$. Wegen $W' \subseteq W$ existieren solche Welten und die entsprechende Kante auch in $\mathcal{M}_3$ und nach Induktionsvoraussetzung gilt $\mathcal{M}_3, v_i \models \phi_i$, also gilt $\mathcal{M}_3, w \models \phi$.

Aus der gezeigten Aussage folgt mit $h(w_2) = 0, d(\varphi) \leq k$ und $\mathcal{M}_3, w_2 \models \varphi$ insbesondere auch $\mathcal{M}_4, w_2 \models \varphi$, sodass $\mathcal{M}_4$ das gewünschte endliche Modell für φ ist. $\square$

4 Temporale Logik

In diesem Kapitel untersuchen wir die beiden CTL^*-Varianten LTL und CTL hinsichtlich der endlichen Modelleigenschaft. Da sich für LTL schnell ein Gegenbeispiel finden lässt, widmet sich der Großteil dieses Kapitels CTL und weist die endliche Modelleigenschaft wie in [2] nach.

4.1 CTL

In einfacher Modallogik hat die modale Tiefe einer Formel stets die Anzahl der sichtbaren Welten auf eine endliche Anzahl beschränkt. Durch dieses sowie durch das gezeigte Quotientenstruktur-Argument konnte schließlich die endliche Modelleigenschaft nachgewiesen werden.

Für CTL existiert keine so intuitive Erklärung, weil durch die eingeführten Pfadformeln keine direkte Einschränkung dafür existiert, welche Welten für eine Formel überhaupt sichtbar sind. Dennoch kann ein ähnliches Argument hinsichtlich Quotientenstrukturen wie bereits im vorherigen Kapitel genutzt werden, um zu zeigen, dass eine erfüllbare CTL-Formel bereits auf einem endlichen Modell erfüllt werden kann und CTL somit die endliche Modelleigenschaft besitzt.

Im Folgenden ist, soweit nicht anders erwähnt, mit *Modell* stets ein Modell für CTL gemeint sowie mit Formelmenge stets eine Formelmenge, bestehend aus CTL-Formeln.

Für eine Formelmenge Φ und ein Modell $\mathcal{M} = (W, R, V)$ defninieren wir $\sim_\Phi$ ebenso wie in Kapitel 3 und können so erneut eine Quotientenstruktur defninieren. Durch die Endlichkeit von $\mathcal{P}(\Phi)$ folgt natürlich wieder die Endlichkeit des entstehenden Quotienten-Modells. Wir werden aber im Folgenden sehen, dass das Modell leider nicht notwendigerweise die Gültigkeit aller Formeln aus Φ beibehält. Weil die nachfolgende Argumentation einen Umweg über Hintikka-Strukturen nimmt, definieren wir Quotientenstrukturen für Modelle in diesem Kapitel direkt über deren kanonische Hintikka-Struktur (Lemma 2.15). Die Schreibweise für Äquivalenzklassen und W_Φ werden aus dem dritten Kapitel übernommen.

Definition 4.1. *Es sei Φ eine Formelmenge sowie $\mathcal{M} = (W, R, L)$ eine Hintikka-Struktur und $\sim_\Phi$ gegeben durch $w \sim_\Phi v :\Leftrightarrow L(w) \cap \Phi = L(v) \cap \Phi$ für $w, v \in W$. Dann heißt*

$$\mathcal{M}^f_\Phi := (W_\Phi, \{(|w|_\Phi, |v|_\Phi) \mid (w, v) \in R\}, L')$$

die Quotientenstruktur von $\mathcal{M}$ durch Φ, wobei $L'(|w|_\Phi) = L(w) \cap \Phi$ für alle $w \in W$.

Für ein Modell $\mathcal{M}$ mit kanonischer Hintikka-Struktur $\mathcal{M}'$ setzen wir $\mathcal{M}^f_\Phi := \mathcal{M}'^f_\Phi$.

In Kapitel 3 haben wir den Abschluss einer Formelmenge unter Teilformeln definiert. Wir verwenden hier eine vergleichbare Definition, die uns eine Art Normalteiler liefert. An dieser Stelle gehen wir jedoch von einer einzelnen Formel ϕ aus und definieren ein Pendant zu $\mathsf{sub}(\phi)$, genannt Fischer-Ladner-Abschluss von ϕ:

Definition 4.2 (Fischer-Ladner-Abschluss)**.** *Sei $\varphi \in \mathsf{FORM}_{\mathsf{CTL}}$. Dann sei $H(\varphi)$ der Durchschnitt aller Mengen H mit*

(1) $\varphi \in H$

(2) $\neg\psi \in H \Rightarrow \psi \in H$

(3) $\phi \wedge \psi \in H \Rightarrow \phi, \psi \in H$

(4) $A[\phi \textit{ until } \psi] \in H \Rightarrow \phi, \psi, AXA[\phi \textit{ until } \psi] \in H$

(5) $AX\phi \in H \Rightarrow \phi \in H$

Es sei $\neg H := \{\neg\phi \mid \phi \in H\}$. *Dann heißt* $\mathsf{FL}(\varphi) := H(\varphi) \cup \neg H(\varphi)$ *der Fischer-Ladner-Abschluss von* φ.

Wenn später über die Endlichkeit der Formelmenge Φ, mit deren Hilfe die Quotientenstruktur konstruiert wird, argumentiert werden soll, ist es natürlich notwendig, dass diese Definition keine unendlichen Formelmengen erschafft. Das nachfolgende Lemma zeigt, dass das auch nicht der Fall ist.

Lemma 4.3. *Sei* $\varphi \in \mathsf{FORM}_{\mathsf{CTL}}$. *Dann ist* $\mathsf{FL}(\varphi)$ *endlich.*

Beweis. Mithilfe von Induktion über die Struktur von φ zeigen wir zunächst, dass $H(\varphi)$ für alle $\varphi \in \mathsf{FORM}_{\mathsf{CTL}}$ endlich ist.

(I.A.) Für alle $\varphi \in \mathsf{VAR}$ gilt $H(\varphi) = \{\varphi\}$.

(I.S.) Es seien $H(\phi), H(\psi)$ endlich. Dann gilt:

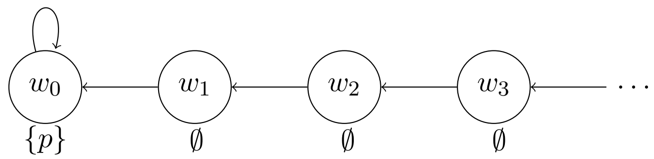
- Für $\varphi = \neg\phi$ ist $\varphi \in H(\varphi)$ und mit (2) $\phi \in H(\varphi)$. Alle Formeln, die wegen $\phi \in H(\varphi)$ in $H(\varphi)$ enthalten sein müssen, sind bereits in $H(\phi)$ enthalten. Es gilt also $H(\varphi) = \{\varphi\} \cup H(\phi)$. Da nach Induktionsvoraussetzung $H(\phi)$ endlich ist, muss auch $H(\varphi)$ endlich sein.
- Für $\varphi = \phi \wedge \psi$ ist $\varphi \in H(\varphi)$ und mit (3) $\phi, \psi \in H(\varphi)$. Analog zum letzten Fall folgt nun $H(\varphi) = \{\varphi\} \cup H(\phi) \cup H(\psi)$ und nach Induktionsvoraussetzung folgt, dass $H(\varphi)$ endlich ist.
- Für $\varphi = A[\phi \text{ until } \psi]$ ist $\varphi \in H(\varphi)$ und mit (4) folgt $\phi, \psi, AX\varphi \in H(\varphi)$. Durch $AX\varphi \in H(\varphi)$ folgt mit (5) lediglich wieder $\varphi \in H(\varphi)$, sodass insgesamt $H(\varphi) = \{\varphi, AX\varphi\} \cup H(\phi) \cup H(\psi)$ gilt. Mit der Induktionsvoraussetzung ist $H(\varphi)$ endlich.
- Für $\varphi = AX\phi$ ist $\varphi \in H(\varphi)$ und mit (5) $\phi \in H(\varphi)$. Wieder folgt analog mit $H(\varphi) = \{\varphi\} \cup H(\phi)$ die Aussage.

Da offensichtlich $|\mathsf{FL}(\varphi)| \leq 2|H(\varphi)|$, folgt die Aussage. □

Speziell kann die Quotienten-Konstruktion die Gültigkeit von until-Formeln, z.B. der Formel AFp (wobei p eine Variable ist), nicht beibehalten, da ggf. neue Zyklen eingeführt werden, sodass Pfade entstehen können, die an Welten, die vorher auf jedem Pfad lagen, vorbeiführen. Ein solcher Zyklus entsteht bei der Konstruktion des Quotientenmodells im folgenden Beispiel.

Beispiel 4.4

Es sei $\varphi := AFp$. Das nachfolgend abgebildete Modell $\mathcal{M}$ hat offenbar die Eigenschaft, dass $\mathcal{M}, w_i \models \varphi$ für alle $i \geq 0$.



Wir betrachten nun $\Phi = \mathsf{FL}(\varphi)$. Da Φ endlich ist, ist auch W_Φ endlich (vgl. Lemma 3.6). Es folgt also die Existenz von $i > j > 0$, sodass $|w_i|_\Phi = |w_j|_\Phi$. Dann gibt es in $\mathcal{M}^f_\Phi$ einen Pfad von $|w_i|_\Phi$ nach $|w_j|_\Phi$, der offenbar nicht $|w_0|_\Phi$ enthält. Da aber $|w_i|_\Phi = |w_j|_\Phi$, handelt es sich bei diesem Pfad um einen Zyklus.

Folglich existiert ein (unendlich langer) Pfad

$$\pi := |w_i|_\Phi, \ldots, |w_j|_\Phi = |w_i|_\Phi, \ldots, |w_j|_\Phi = |w_i|_\Phi, \ldots,$$

der von $|w_i|_\Phi$ ausgeht und der $|w_0|_\Phi$ nicht enthält, also auch keine Welt, in der p gilt, d.h. $\mathcal{M}^f_\Phi, \pi \not\models Fp$. Daraus folgt aber $\mathcal{M}^f_\Phi, |w_i|_\Phi \not\models AFp$ – im Gegensatz zu $\mathcal{M}, w_i \models AFp$.

Wir sind also nicht in der Lage, Eigenschaften wie in Lemma 3.5 für das Quotientenmodell nachzuweisen. Stattdessen werden wir im Folgenden einige schwächere Eigenschaften nachweisen und schließlich aus dem Quotientenmodell durch geeignete Modifikationen, die die Endlichkeit des Modells beibehalten, ein Modell konstruieren, das die Gültigkeit ausgewählter Formeln aus dem ursprünglichen Modell gewährleistet.

Wie in Beispiel 4.4 gezeigt wurde, gilt (H9) in Quotientenstrukturen im Allgemeinen nicht. Der Grund dafür waren neu entstehende Zyklen im Quotientenmodell. Eine naheliegende Überlegung ist daher, aus der Quotientenstruktur die verantwortlichen Kanten zu entfernen, um die störenden Zyklen zu eliminieren.

Gleichzeitig soll die Struktur, die durch das Entfernen von Kanten entsteht, im Quotientenmodell enthalten sein, das heißt, es sollen weder neue Kanten noch neue Welten hinzugefügt werden, sondern lediglich selbige entfernt werden. Wir erhalten die folgende Definition:

Definition 4.5. *In einem gerichteten, azyklischen Graphen ist ein innerer Knoten ein Knoten, der mindestens einen Nachfolger hat, während ein Randknoten ein Knoten ohne Nachfolger ist. Im Zusammenhang mit Rahmen verwenden wir auch die Terminologie innere Welt bzw. Randwelt.*

Eine Struktur $\mathcal{M} = (W, R, L)$, deren Rahmen ein gerichteter, azyklischer Graph ist, heißt Fragment, falls (H1)-(H8) in allen inneren Welten von $\mathcal{M}$ gilt und (H1)-(H6) in allen Randwelten von $\mathcal{M}$ gilt.

$\mathcal{M}_1 = (W_1, R_1, L_1)$ heißt enthalten in $\mathcal{M}_2 = (W_2, R_2, L_2)$, geschrieben $\mathcal{M}_1 \subseteq \mathcal{M}_2$, falls $W_1 \subseteq W_2$, $R_1 \subseteq R_2$ und $L_1(w) = L_2(w)$ für alle $w \in W_1$.

$\mathcal{M}_1$ heißt eingebettet in $\mathcal{M}_2$, in Zeichen $\mathcal{M}_1 \leq \mathcal{M}_2$, falls $\mathcal{M}_1 \subseteq \mathcal{M}_2$ und für jede Kante $(w, v) \in R_2 \cap (W_1 \times W_2 \backslash W_1)$ gilt: w ist eine Randwelt in $\mathcal{M}_1$.

Mit anderen Worten heißt der letzte Teil der Definition, dass jede Kante, die aus dem eingebetteten Modell herausführt, in einer Randwelt des eingebetteten Modells beginnen muss. Damit wird erzwungen, dass jeder Pfad von einer Welt in $\mathcal{M}_2$ zu einer nicht zu $\mathcal{M}_2$ gehörigen Welt durch eine Randwelt von $\mathcal{M}_2$ führen muss.

Lemma 4.6. *Es seien $\mathcal{M} = (W, R, L)$ eine Hintikka-Struktur für $\varphi \in \mathsf{FORM}_{\mathsf{CTL}}$ und $w \in W$. Sei außerdem $M' = (W', R', L')$ mit $M' := \mathcal{M}^f_\Phi$ für $\Phi = \mathsf{FL}(\varphi)$. Falls $A[\phi \text{ until } \psi] \in L(|w|_\Phi)$, dann existiert ein Fragment $N \subseteq M'$ mit Wurzel $|w|_\Phi$, sodass $\psi \in L(v)$ für alle Grenzwelten v von N gilt und $\phi \in L(u)$ für alle inneren Knoten u von N.*

Beweis. Wir definieren $\hat{L}(w) = L(w) \cap \Phi$ für alle $w \in W$.

Behauptung 1: Wir können o.B.d.A. annehmen, dass alle Welten in W nur endlich viele Nachfolger haben.

Beweis. Falls es eine oder mehrere Welten mit unendlich vielen Nachfolgern gibt, konstruieren wir ein endliches Modell $\hat{M}$, für das wir die nachfolgende Konstruktion durchführen können, folgendermaßen:

Sei v ein Knoten mit unendlich vielen Nachfolgern. Für alle φ der Form $\neg A\phi$ in $\hat{L}(v)$ wähle eine Kante $(v, v') \in R$, sodass $\neg\phi \in L(v')$. Eliminiere alle nicht gewählten Kanten und die dann nicht mehr erreichbaren Welten. Nach endlich vielen Schritten haben alle Welten nur noch endlich viele Nachfolger (da wegen (H9) keine unendlich langen Pfade existieren können und für jeden Knoten der Prozess nur für endlich viele Nachfolger wiederholt werden muss).

Die Gültigkeit von (H9) ist durch diese Modifikation unberührt, da keine der Bedingung widersprechenden Pfade hinzugefügt werden.

Behauptung 1 □

Es sei $w \in |w|_\Phi$. Da $A[\phi \text{ until } \psi] \in L(w)$ gelten muss, gibt es mit (H9) für jeden Pfad $x = x_0, x_1, \ldots$, der von w ausgeht, ein $i \geq 0$, sodass $\psi \in L(x_i)$ und $\phi \in L(x_j)$ für $0 \leq j < i$. Wir konstruieren $M_0 = (W_0, R_0, L_0)$, indem wir fordern, dass W_0 minimal ist, sodass für jeden solchen Pfad gilt, dass $x_0, \ldots, x_i \in W_0$. Zudem gelte für jeden solchen Pfad $(x_k, x_{k+1}) \in R_0$ für alle $0 \leq k < i$, falls $x_j \neq x_l$ für alle $j \neq l$ mit $j, l \leq i$. Setze $L_0(t) = \hat{L}(t)$ für alle $t \in W_0$.

Wir beobachten:

- M_0 ist azyklisch, da alle Welten, in denen ψ erfüllt ist, nach Konstruktion keinen Nachfolger haben. Wenn M_0 nun einen Zyklus enthält, dann ist dieser auch schon in $\mathcal{M}$ enthalten gewesen und er enthält insbesondere keine Welt, in der ψ gilt. Entgegen der Voraussetzung gibt es dann aber einen unendlichen Pfad, der keine Welt enthält, in der ψ erfüllt ist.
- M_0 ist endlich, da nach Voraussetzung alle Knoten in W_0 nur endlich viele Nachfolger haben und nach dem Lemma von König (Lemma 2.3) ein unendlich langer Pfad in M_0 existieren würde, falls M_0 unendlich wäre. Das stünde jedoch im Widerspruch zu (H9).

Damit ist M_0 ein Fragment.

Behauptung 2: Wir können aus M_0 in endlich vielen Schritten ein Fragment $M_k = (W_k, R_k, L_k)$ konstruieren, sodass für alle $v, w \in W_k$ gilt: $w = v$ oder $L_k(w) \neq L_k(v)$.

Beweis. Falls bereits $w = v$ oder $L_0(w) \neq L_0(v)$ für alle $w, v \in W_0$ gilt, ist nichts zu zeigen.

Anderenfalls gibt es $w \neq v \in W_i$ (o.B.d.A. sei $d(v) \leq d(w)$), sodass $L_i(w) = L_i(v)$ und wir konstruieren $M_{i+1} = (W_{i+1}, R_{i+1}, L_{i+1})$ aus M_i wie folgt:

- Setze $W_{i+1} := W_i$ und $R_{i+1} := R_i$.
- Für alle $u \in W_i$ mit $(u, v) \in R_i$ ersetze (u, v) durch (u, w) in R_{i+1}. Entferne v aus W_{i+1}.
- Entferne alle von der Wurzel aus nicht mehr erreichbaren Welten aus W_{i+1}.
- Setze $L_{i+1}(w) := L_i(w)$ für alle $w \in W_{i+1}$.

Dann gilt $|W_{i+1}| < |W_i|$. Nach endlich vielen Schritten (aufgrund der Endlichkeit von M_0) erhalten wir so M_k. Die Eigenschaften von M_0 bzgl. der Gültigkeit von ϕ und ψ wurden offensichtlich beibehalten.

Behauptung 2 $\square$

Dann können wir $M'_k := (W'_k, R'_k, L'_k)$ mit $W'_k = \{|w|_\Phi \mid w \in W_k\}$, $R'_k = \{(|w|_\Phi, |v|_\Phi) \mid (w, v) \in R_k\}$ und $L'_k(|w|_\Phi) = L_k(w)$ für alle $w \in W_k$ definieren und dafür nachweisen, dass $M'_k \subseteq M'$:

Es gilt $L'_k(|w|_\Phi) = \hat{L}(w) = L(w) \cap \Phi = L'(|w|_\Phi)$ für alle $w \in W_k$. Außerdem gilt $(|w|_\Phi, |v|_\Phi) \in R'_k \Rightarrow (w, v) \in R_k \Rightarrow (w, v) \in R \Rightarrow (|w|_\Phi, |v|_\Phi) \in R'$, woraus $R'_k \subseteq R'$ folgt. Da auch offenbar $W'_k \subseteq W'$ gilt, folgt $M'_k \subseteq M'$. Aufgrund von $w \neq v \Rightarrow L_k(w) \neq L_k(v) \Rightarrow |w|_\Phi \neq |v|_\Phi$ ist M'_k zudem weiterhin ein Fragment (mit der Wurzel $|w|_\Phi$) und damit insgesamt von der gewünschten Form.

$\square$

Schließlich können wir mit Hilfe der vorherigen Aussagen präzisieren, welche Eigenschaften die Quotientenkonstruktion beibehält. Die entstehende Struktur halten wir mit der folgenden Definition fest.

Definition 4.7 (Pseudo-Hintikka-Struktur). *Eine Pseudo-Hintikka-Struktur ist ein Tripel $\mathcal{M} = (W, R, L)$, sodass für alle $w \in W$ die Axiome (H1) bis (H8) gelten sowie*

(H9') *$A[\phi \text{ until } \psi] \in L(w) \Rightarrow$ es existiert ein Fragment $N \subseteq \mathcal{M}$ mit Wurzel w, sodass $\psi \in L(v)$ für alle Randwelten v von N gilt sowie $\phi \in L(u)$ für alle inneren Welten in N.*

In einer Pseudo-Hintikka-Struktur (W, R, L) heißt eine Formel φ der Form $A[\phi \text{ until } \psi]$ in einer Welt $w \in W$ konsistent, falls $\varphi \in L(w)$ und $(H9)$ für φ in w erfüllt ist.

Satz 4.8. *Es sei $\mathcal{M}$ eine Hintikka-Struktur, $\varphi \in \mathsf{FORM}_{\mathsf{CTL}}$ und $\Phi = \mathsf{FL}(\varphi)$. Dann ist $\mathcal{M}^f_\Phi$ eine Pseudo-Hintikka-Struktur.*

Beweis. Wir weisen die Gültigkeit der Axiome (H1)-(H8) sowie (H9') in $\mathcal{M}^f_\Phi$ nach. Sei dafür $\mathcal{M} = (W, R, L)$ und $\mathcal{M}' = \mathcal{M}^f_\Phi = (W', R', L')$.

$(*)$ Falls für ein $w' \in W'$ $\phi, \psi \in L'(w')$ gilt, gibt es ein $w \in W$, sodass $\phi, \psi \in L(w)$, da sowohl $\phi, \psi \in \Phi$ durch die Definition $L'(|w|_\Phi) = \Phi \cap L(w)$ folgt.

Im Folgenden gilt $w' \in W'$.

(H1) Es gelte $\phi \in L'(w')$. Daraus folgt nach Definition von $\mathcal{M}'$, dass $\phi, \neg\phi \in \Phi$, weil Φ ein Fischer-Ladner-Abschluss ist. Angenommen, es gilt nun $\neg\phi \in L'(w')$, dann gibt es nach $(*)$ ein $w \in W$, sodass $\phi, \neg\phi \in L(w)$, allerdings verletzt $\mathcal{M}$ dann (H1). Es folgt also $\neg\phi \notin L'(w')$.

(H2)-(H6) Wir zeigen nur die Gültigkeit von (H2), da die Gültigkeit der anderen Axiome analog gezeigt werden kann. Es gelte $\neg\neg\phi \in L'(w')$. Dann gilt $\neg\neg\phi \in L(w)$ für ein $w \in W$ und mit (H2) gilt $\phi \in L(w)$. Es gilt nun $\neg\neg\phi \in \Phi \Rightarrow \phi \in \Phi$, sodass $\phi \in L'(w')$ folgt.

(H7) Es gelte $AX\phi \in L'(w')$. Für alle $v' \in W'$ mit $(w', v') \in R'$ gibt es nach Konstruktion von R' ein $v \in W$, sodass $(w, v) \in R$ für ein $w \in W$ mit $\phi \in L(w)$. Für jede solche Kante folgt mit (H7) dann $\phi \in L(v)$ und schließlich wegen $\phi \in \Phi$, dass $\phi \in L(v')$ und damit die Gültigkeit von (H7) in $\mathcal{M}'$.

(H8) Es gelte $\neg AX\phi \in L'(w')$. Dann gibt es ein $w \in W$ mit $\neg AX\phi \in L(w)$. Mit (H8) folgt, dass es ein $v \in W$ mit $(w, v) \in R$ und $\neg\phi \in L(v)$ gibt. Da $\neg\phi \in \Phi$ gelten muss, folgt: $\neg\phi \in L'(|v|_\Phi)$ und aus der Konstruktion von R' folgt $(w', |v|_\Phi) \in R'$.

(H9') Folgt direkt aus dem vorherigen Lemma.

□

Durch Satz 4.8 erfahren wir, dass wir für das Quotientenmodell *nur eine* zusätzliche Eigenschaft benötigen, um zu zeigen, dass die Gültigkeit aller Formeln aus Φ in einem endlichen Modell beibehalten werden kann. Wir haben gesehen, dass lediglich until-Formeln ihre Gültigkeit ändern können. Die folgenden Aussagen führen uns nun schrittweise zu einem Modell, das wir aus dem Quotientenmodell konstruieren, um auch die Gültigkeit von (H9) wiederherzustellen. Dabei werden wir nur einen endlichen Blow-Up erhalten, sodass die herbeigeführte Behauptung genügt, um schließlich ein endliches Modell anzugeben, das die Gültigkeit aller im ursprünglichen Modell geltenden Formeln beibehält.

Lemma 4.9. *Es sei N ein Fragment, $\varphi = A[\phi \text{ until } \psi]$ für $\phi, \psi \in \mathsf{FORM}_{\mathsf{CTL}}$ und w eine Welt in N mit $\varphi \in L(w)$. Dann gilt für jeden Pfad $x = x_0, x_1, \ldots, x_k$ von $w = x_0$ zu einer Randwelt $t = x_k$ in N entweder*

(1) es existiert ein $0 \leq i \leq k$, sodass $\psi \in L(x_i), \phi \in L(x_j)$ für alle $0 \leq j < i$ oder

(2) $\phi, A[\phi \text{ until } \psi] \in L(x_i)$ für alle $0 \leq i \leq k$.

Falls $N \leq M$ und φ in M für alle Randwelten von N konsistent ist, dann ist φ für w in M konsistent.

Beweis. Wir beweisen zunächst die erste Aussage des Lemmas.

Sei $\pi = x_0, x_1, \ldots, x_k$ ein Pfad von $w = x_0$ zu einer Randwelt $v = x_k$. Wir zeigen per Induktion über die Teilpfade $x_0, x_1, \ldots, x_i$, dass das Lemma für alle i gilt.

(I.A.) Falls w eine Randwelt in N ist, so folgt die Aussage direkt aus (H5). Andernfalls gilt mit (H5) wegen $\varphi \in L(w)$, dass entweder $\psi \in L(w)$ (dann ist (1) erfüllt) oder $\phi, AX\varphi \in L(w)$. Insgesamt gilt dann aber $\phi, \varphi \in L(w)$, wodurch (2) erfüllt wird.

(I.S.) Es gelte (1) oder (2) für den Teilpfad $\pi_i = x_0, x_1, \ldots, x_i$. Falls (1) für π_i gilt, dann existiert ein $0 \leq j \leq i$, sodass $\psi \in L(x_j), \phi \in L(x_l)$ für alle $0 \leq l < j$. Offenbar gilt dies für den Pfad $x_0, x_1, \ldots, x_{i+1}$ immer noch.

Falls nicht (1), aber (2) für π_i gilt, dann gilt $\phi, \varphi \in L(x_j)$ für alle $0 \le j \le i$. Insbesondere gilt also $\varphi \in L(x_i)$ und mit (H5) auch $AX\varphi \in L(x_i)$ (da $\psi \notin L(x_i)$, weil sonst (2) erfüllt wäre). Da x_i eine innere Welt ist, ist (H7) erfüllt, d.h. es gilt $\varphi \in L(x_{i+1})$. Wiederum mit (H5) folgt dann aber entweder $\psi \in L(x_{i+1})$, wodurch (1) erfüllt wäre, oder $\phi, \varphi \in L(x_{i+1})$. Da bereits $\phi, \varphi \in L(x_j)$ für alle $0 \le j \le i$, gilt insgesamt $\phi, \varphi \in L(x_l)$ für alle $0 \le l \le i+1$ und π_{i+1} erfüllt (2).

Für den zweiten Teil der Aussage prüfen wir, dass (H9) für φ in w erfüllt sein muss. Da $N \le M$, muss jeder von w ausgehende Pfad, der Welten aus M enthält, eine Randwelt von N enthalten. Mit dem ersten Teil des Lemmas folgt, dass auf allen Pfaden zu Randwelten von N entweder (1) oder (2) gelten muss. Für alle Pfade zu Randwelten, auf denen (1) erfüllt ist, sind die Voraussetzungen für $(H9)$ bereits erfüllt. Wir betrachten nun also Pfade zu Randwelten v, auf denen (1) nicht gilt. Da dann (2) auf diesen Pfaden gilt, muss insbesondere auch $\phi, A[\phi \text{ until } \psi] \in L(v)$ gelten. Weil φ in v nach Voraussetzung konsistent ist, muss auf jedem von v ausgehenden Pfad $v, x_1, \ldots$ ein i wie in $(H9)$ existieren. Für jeden Pfad $w, x_1, \ldots, x_{k-1}, v, x_{k+1}, \ldots$ ist die Bedingung von $(H9)$ dann ebenfalls erfüllt : Setze $j = k + i$. Dann gilt $\phi \in L(x_l)$ für alle $0 \le l < j$ und $\psi \in L(x_j)$.

Damit gilt auf allen von w ausgehenden Pfaden in M die Voraussetzung für $(H9)$, also ist φ in w konsistent. □

Falls für eine Formel auf allen Pfaden (1) des Lemmas gilt, ist das nach Definition äquivalent dazu, dass die Formel in w konsistent ist.

Um Quotientenstrukturen im Folgenden so umbauen zu können, dass im entstehenden Modell schließlich wieder alle Formeln konsistent sind, gehen wir nun schrittweise vor. Zunächst konstruieren wir im nächsten Lemma für jede einzelne Welt ein Fragment, in dessen Wurzel alle Formeln konsistent sind.

Anschließend setzen wir diese Fragmente in Lemma 4.12 so zusammen, dass schließlich alle Formeln in allen Welten konsistent sind.

Lemma 4.10. *Es sei $\mathcal{M} = (W, R, L)$ eine endliche Pseudo-Hintikka-Struktur mit $w \in W$. Dann existiert ein endliches Fragment $\mathsf{FRAG}(w)$ mit Wurzel w, sodass alle Formeln der Form $A[\phi \text{ until } \psi]$ in $L(w)$ für w in $\mathsf{FRAG}(w)$ konsistent sind.*

Beweis. Es seien $\varphi_1, \ldots, \varphi_n$ alle Formeln der Form $A[\phi \text{ until } \psi]$ in $L(w)$. Wir definieren zunächst ein Fragment $M_0 = (W_0, R_0, L_0)$ mit Wurzel w und $L_0(w) = L(w)$. Die Konstruktion funktioniert wie folgt:

- Für jede Formel der Form $\neg AX\phi \in L(w)$ füge eine Welt v mit $\neg\phi \in L(v)$ zu W_0 hinzu, ergänze die Kante (w, v) zu R_0.
- Für jede so hinzugefügte Welt v stelle sicher, dass $\phi \in L(v)$ für alle Formeln der Form $AX\phi \in L(w)$.

Da $|L(w)|$ nach Voraussetzung endlich ist, wird so nur eine endliche Anzahl an Welten hinzugefügt. Zudem ist M_0 ein Fragment, da nach Konstruktion (H7) und (H8) in w erfüllt sind. Dass (H1) bis (H6) für alle $v \in W_0$ erfüllt sind, kann durch eine entsprechende Konstruktion der $L(v)$ problemlos erreicht werden.

Wir erweitern das Fragment nun schrittweise, sodass $\varphi_1, \ldots, \varphi_n$ in w konsistent sind. Dafür konstruieren wir eine Folge $M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k = F(w)$, sodass $\varphi_1, \ldots, \varphi_i$ für w in M_i konsistent sind. Wir konstruieren M_{i+1} aus M_i wie folgt:

Es seien $v_1, \dots, v_k$ alle Randwelten in M_i, sodass $\varphi_{i+1} \in L(v_j)$ für alle $j = 1, \dots, k$. Ersetze alle v_j durch ein endliches Fragment N_j mit Wurzel v_j, sodass φ_{i+1} für v_j in N_j konsistent ist, um M_{i+1} zu erhalten.

Da M_i nur endlich viele Randwelten hatte und für jede Randwelt nur endlich viele Welten hinzugefügt wurden, ist auch M_{i+1} endlich. Weiterhin gilt nach Lemma 4.9, dass φ_{i+1} konsistent für w in M_{i+1} ist.

Es folgt, dass M_k die gewünschten Eigenschaften hat. □

Beispiel 4.11

Für eine Welt w in einer Pseudo-Hintikka-Struktur gelte $p, q, \neg r \in L(w)$ sowie $AXq, EXp \in L(w)$ und $AFp, A[q \text{ until } \neg p] \in L(w)$. Es enthalte Φ genau diese Formeln.

Wegen (H5) muss minimal $AXA[q \text{ until } \neg p]$ in $L(w)$ enthalten sein. Hingegen ist es nicht erforderlich, dass $AXAFp \in L(w)$, da $p \in L(w)$.

Im Folgenden bezeichne $\langle\Psi\rangle$ für eine Formelmenge Ψ den Durchschnitt aller Mengen, die Ψ enthalten und (H1) bis (H6) erfüllen.

Das Fragment M_0 aus dem vorherigen Beweis ist gegeben durch:

$$\begin{array}{ccc} w & \longrightarrow & w_1 \\ \langle\Phi\rangle & & \langle\Phi_1\rangle \end{array}$$

Dabei ist $\Phi_1 = \{p, q, A[q \text{ until } \neg p]\}$. Es gibt nun zwei Formeln, deren Konsistenz in w wir sicherstellen müssen: AFp und $A[q \text{ until } \neg p]$. Wir beginnen mit AFp. Da $p \in L(w)$, ist die Formel bereits konsistent in w, sodass wir $M_1 = M_0$ setzen können.

Für die Konstruktion von M_2 stellen wir fest, dass es keinen von w ausgehenden Pfad gibt, auf dem irgendwann $\neg p$ gilt, d.h. die Formel ist nicht konsistent in w. Wir ersetzen daher alle Randwelten unseres Fragments M_1 durch Fragmente, in deren Wurzel $A[q \text{ until } \neg p]$ konsistent ist.

In unserem Fall haben wir nur w_1 zu ersetzen und können einfach das folgende Fragment N finden:

$$\begin{array}{ccc} w_1 & \longrightarrow & w_2 \\ \langle\Phi_1\rangle & & \langle\{\neg p\}\rangle \end{array}$$

Durch Ersetzen von w_1 durch N in M_1 erhalten wir schließlich das Fragment M_2, in dem alle Formeln in w konsistent sind.

Wir starten nun mit einer Pseudo-Hintikka-Struktur für eine Formel φ und konstruieren mithilfe von Lemma 4.10 ein Fragment, in dessen Wurzel φ konsistent ist. Die nachfolgende Konstruktion stellt die Konsistenz nun auch für alle weiteren Welten der entstehenden Struktur her, ohne dabei unendlich viele Welten hinzuzufügen. Aus dem folgenden Lemma erhalten wir deswegen sofort die endliche Modelleigenschaft von CTL (Satz 4.13).

Lemma 4.12. *Sei $\mathcal{M} = (W, R, L)$ eine endliche Pseudo-Hintikka-Struktur für φ. Dann existiert eine endliche Hintikka-Struktur $\mathcal{M}'$ für φ.*

Beweis. Offenbar ist auch $\hat{\mathcal{M}} := (W, R, \hat{L})$ mit $\hat{L}(w) = \mathsf{FL}(\varphi) \cap L(w)$ eine Pseudo-Hintikka-Struktur. Wir konstruieren $\mathcal{M}'$ induktiv wie folgt:

Sei $w \in W$ mit $\varphi \in L(w)$. Dann setze $M_1 := \mathsf{FRAG}(w)$.

Sei $M_i = (W_i, R_i, L_i)$ und seien $w_1, \ldots, w_k$ alle Randwelten von M_i (diese Liste muss endlich sein, da M_i endlich ist). Wir erhalten nun M_{i+1} aus M_i, indem wir für alle $w_j, 1 \leq j \leq k$ Folgendes tun:

- Falls es eine innere Welt $w' \in W_i$ gibt, sodass $L_i(w') = L_i(w_j)$ und w' die Wurzel eines in M_i eingebetteten Fragments $\mathsf{FL}(w')$ ist, dann ersetze alle Kanten der Form $(v, w_j) \in R_i$ durch (v, w') und entferne w_j.
- Ansonsten ersetze w_j durch $\mathsf{FRAG}(w_j)$.

Das so entstehende Modell $(W_{i+1}, R_{i+1}, L_{i+1})$ ist M_{i+1}.

Behauptung: Nach endlich vielen Schritten sind keine Randwelten mehr vorhanden.

Beweis. Für wie beschrieben konstruierte $M_n = (W_n, R_n, L_n)$ gilt: $L_n(w) \subseteq \mathsf{FL}(\varphi)$ für alle $w \in W_n$ (und damit gibt es mit Lemma 4.3 nur endlich viele verschiedene Möglichkeiten, wie $L_n(w)$ aussehen kann). Sei also $|\mathsf{FL}(\varphi)| = m$. Für alle M_n setze

$$A_n := \{X \subseteq \mathcal{P}(\mathsf{FL}(\varphi)) \mid \text{Es existiert eine innere Welt } v \in W_n \text{ mit } L_n(v) = X, \\ \text{die Wurzel eines Fragments } \mathsf{FL}(v) \leq M_n \text{ ist}\}.$$

Für eine Randwelt $w \in W_n$, die in der Konstruktion von M_{n+1} nicht durch eine innere Welt ersetzt wird, gilt nach Konstruktion $L_n(w) \notin A_n$ (falls eine solche Welt für M_n nicht existiert, besitzt M_{n+1} bereits keine Randwelten mehr und wir sind fertig). Falls eine solche Ersetzung für die Konstruktion von M_{n+1} vorgenommen werden muss, gilt $A_n \subsetneq A_n \cup L(w) \subseteq A_{n+1}$, also auch $|A_n| < |A_{n+1}|$. Da nun aber $|A_n| \leq |\mathcal{P}(\mathsf{FL}(\varphi))| = 2^m$ für alle $n \in \mathbb{N}$ gilt, muss es ein $n \in \mathbb{N}$ geben, sodass $|A_n| = |A_x|$ für alle $x \geq n$ gilt. Daraus folgt aber, dass M_n keine Randwelten v besaß, für die $L(v) \notin A_n$ galt. Folglich werden alle solchen v bei der Konstruktion von M_{n+1} durch innere Welten ersetzt und M_{n+1} besitzt keine Randwelten. Behauptung □

Sei also k minimal, sodass M_k keine Randwelten hat. Dann setze $\mathcal{M}' := M_k$. $\mathcal{M}'$ ist dann die gewünschte Hintikka-Struktur, wie wir im Folgenden nachprüfen.

Da die Konstruktion nach endlich vielen Schritten endet und in jedem Schritt nur endlich viele endliche Fragmente hinzugefügt werden können, muss auch $\mathcal{M}'$ endlich sein.

$(H1)$ bis $(H8)$ sind trivial dadurch erfüllt, dass während der Konstruktion nur Fragmente zusammengesetzt werden und Randwelten immer im nächsten Konstruktionsschritt durch innere Welten ersetzt wurden, in denen nach der Definition von Fragmenten $(H7)$ und $(H8)$ erfüllt ist.

Sei $w \in W_k$ und $\varphi \in L_k(w)$ eine Formel der Form $A[\phi \text{ until } \psi]$.

Nach Konstruktion von M_k ist w eine Welt eines Fragments $N \leq M_k$ der Form $N = \mathsf{FRAG}(v)$ für ein $v \in W_k$. Mit Lemma 4.9 folgt, dass für jede Randwelt v von N, für die (2) aus Lemma 4.9 nicht gilt, $\varphi \in L_k(v)$. Jedes solche v muss nun wiederum die Wurzel eines Fragments $\mathsf{FRAG}(v)$ sein (weil v in der Konstruktion entweder durch das entsprechende Fragment ersetzt wurde oder mit der Wurzel eines bereits bestehenden Fragments $\mathsf{FRAG}(v)$ gleichgesetzt wurde). Daraus folgt, dass φ für v in $\mathsf{FRAG}(v)$ und mit Lemma 4.9 auch in M_k konsistent ist. Schließlich folgt mit dem selben Lemma, dass φ für w in M_k konsistent sein muss. M_k erfüllt also in allen Welten $(H9)$. □

Satz 4.13. *Es sei $\varphi \in \mathsf{FORM}_{\mathsf{CTL}}$ erfüllbar auf einem beliebigen Modell $\mathcal{M}$. Dann existiert ein endliches Modell, in dem φ erfüllbar ist.*

Beweis. Mit Lemma 2.15 folgt, dass es eine Hintikka-Struktur $\mathcal{M}_H$ für φ gibt. Dann ist ${\mathcal{M}_H}^f_{\mathsf{FL}(\varphi)}$ eine endliche Pseudo-Hintikka-Struktur für φ. Schließlich folgt mit Lemma 4.12, dass es dann auch eine endliche Hintikka-Struktur für φ gibt. Wiederum mit Lemma 2.15 ist φ dann erfüllbar für ein endliches Model. □

4.2 LTL

In diesem Abschnitt untersuchen wir schließlich, ob LTL die endliche Modelleigenschaft besitzt. Wir gehen dabei von der Erkenntnis aus dem dritten Kapitel aus, dass die einfache Modallogik die endliche Modelleigenschaft nicht besitzt, wenn man die Klasse der erlaubten Rahmen auf transitive, irreflexive Rahmen einschränkt. Auf diese Weise wurde auch gefolgert, dass die einfache temporale Logik die endliche Modelleigenschaft nicht besitzt.

Da LTL-Formeln ausschließlich auf Pfaden $x = x_0, x_1, \ldots$ ausgewertet werden und bei Auswertung einer Formel für x^i stets alle x_j mit $j < i$ unsichtbar sind, können wir mit LTL keine Zyklen realisieren. Die Abwesenheit von Zyklen war im dritten Kapitel ein wichtiges Argument für die Notwendigkeit unendlicher Modelle.

Auch so etwas wie Transitivität lässt sich für die lineare temporale Logik finden. Im Wesentlichen war hier das Argument, dass eine Welt bereits all ihre Nachfolgerwelten sieht, sodass es möglich ist, für ausnahmslos alle Nachfolgerwelten bestimmte Eigenschaften zu erzwingen. Vergleichbar ist die Pfadformel $A[\phi \text{ until } \psi]$, bei der beliebig weit in die Zukunft geblickt werden kann.

Wir geben nun ein zum dritten Kapitel analoges Beispiel an, das zeigt, dass LTL die endliche Modelleigenschaft im Allgemeinen nicht besitzt.

Satz 4.14. LTL *besitzt die endliche Modelleigenschaft nicht.*

Beweis. Es sei p eine Variable. Die Formel $\varphi = Xp \wedge GXp$ ist auf dem folgenden Pfad erfüllt.

$$\begin{array}{ccccccc} x_0 & \longrightarrow & x_1 & \longrightarrow & x_2 & \longrightarrow & \cdots \\ \{p\} & & \{p\} & & \{p\} & & \end{array}$$

Wir zeigen nun, dass ein Pfad, der φ erfüllt, unendlich sein muss. Es sei also $\pi = (x, V)$ beliebig, sodass $\pi, i \models \varphi$ für ein i. Angenommen, π ist endlich. Weil π endlich ist, muss es ein $k \geq i$ geben, sodass $x = x_0, x_1, \ldots, x_k$. Insbesondere muss $k > i$ gelten, da sonst $\pi, i \not\models Xp$ (d.h. i hätte keinen Nachfolger). Wegen $k > i$ und $\pi, i \models GXp$ muss nun aber $\pi, k \models Xp$ gelten, d.h. $\pi, k+1 \models p$ muss gelten. Da k aber keinen Nachfolger hat, ist das ein Widerspruch zur Annahme. Folglich muss π unendlich sein. $\square$

5 Zusammenfassung

In dieser Arbeit haben wir einen allgemeineren Begriff für Modallogik eingeführt und gesehen, dass dieser die endliche Modelleigenschaft besitzt. Für den Nachweis haben wir über Bisimulationen bzw. alternativ über die Filtrierung – ein spezielles Quotientenmodell – argumentiert.

Mit der Konstruktion von Quotientenmodellen wurde eine elegante und mächtige Methode, die endliche Modelleigenschaft von verschiedenen Logiken nachzuweisen, vorgestellt. Hier konnte mit dieser Technik für die einfache Modallogik sowie für die *Computation Tree Logic* CTL die endliche Modelleigenschaft nachgewiesen werden, möglich ist aber z.B. auch eine Anwendung auf die dynamische Logik PDL [2]. Darüber hinaus gibt es noch eine Vielzahl weiterer Logiken, für die die Anwendbarkeit der präsentierten Methode geprüft werden kann.

Am Beispiel einfacher Modallogik konnte im dritten Kapitel ein direkter Zusammenhang zwischen endlicher Modelleigenschaft und Entscheidbarkeit modaler Logik hergestellt werden. In [2] wird außerdem gezeigt, wie auch für CTL ein vergleichbares Ergebnis herbeigeführt werden kann. Es wurde angedeutet, dass die in Kapitel 3 formulierte obere Schranke für die Größe von Modellen relativ schlecht ist (vgl. Seite 19), sodass es naheliegt, dass sich bessere obere Schranken finden und beweisen lassen.

Für das Model Checking sind solche Ergebnisse essentiell, um die Laufzeit von Verifikationsalgorithmen für Programme zu beschränken. Die endliche Modelleigenschaft kann aber auch als eine Schwäche modaler Logik aufgefasst werden, da sie nicht in der Lage ist, unendliche Modelle durch das Aufstellen entsprechender Formeln zu erzwingen (vgl. [1]). Dadurch unterscheidet sie sich beispielsweise von der Prädikatenlogik, durch die sich unendliche Trägermengen vergleichsweise einfach erzwingen lassen. Es ist insofern interessant, die Formalisierbarkeit durch verschiedene Modallogiken zu untersuchen und z.B. mit der Prädikaten- oder Aussagenlogik zu vergleichen.

Darüber hinaus haben wir gesehen, dass beim Analysieren der endlichen Modelleigenschaft die Klasse der erlaubten Rahmen eine Rolle spielt – so konnte mithilfe der Filtrierung in Kapitel 3 z.B. kein Ergebnis für transitive Rahmen hergeleitet werden, wohl aber für symmetrische bzw. reflexive Rahmen. Aus unseren Überlegungen ergab sich schließlich, dass die einfache temporale Logik und analog die *Linear Temporal Logic* LTL nicht ohne unendliche Modelle auskommen. Als hinreichende Eigenschaft zum Widerlegen der endlichen Modelleigenschaft haben wir an dieser Stelle die Kombination aus Transitivität und Irreflexivität charakterisiert.

Literaturverzeichnis

[1] P. Blackburn, M. de Rijke, and Y. Venema. *Modal logic.* Cambridge University Press, 2001.

[2] E. Emerson and J. Halpern. Decision procedures and expressiveness in the temporal logic of branching time. *Journal of Computer and System Sciences*, 30:1–24, 1985.

[3] J. Esparza and K. Heljanko. Model checking ltl. *Unfoldings*, pages 125–149, 2008.

[4] Dov M. Gabbay, A. Kurucz, F. Wolter, and M. Zakharyaschev. *Many-dimensional modal logics: theory and applications.* Elsevier, 2003.

[5] A. Meier. *On the Complexity of Modal Logic Variants and their Fragments.* 2011.

[6] K. Rozier and M. Vardi. Ltl satisfiability checking. *International Journal on Software Tools for Technology Transfer*, 12:123–137, 2010.

[7] Wikipedia. König's lemma. `https://en.wikipedia.org/wiki/K%C5%91nig%27s_lemma`, 16. Juli 2020.