Quantitative Analyse Probabilistischer Systeme

Marcus Größer
Institut für Informatik I
Universität Bonn

Bonn, den 21.06.2002

Inhaltsverzeichnis

Kapitel 1

Einleitung

Heutzutage spielen Computersysteme eine immer größer werdende Rolle in unserem Alltagsleben. In fast jedem Bereich werden Computer eingesetzt, seien es elektronische Bremsassistenten in Autos, Geldautomaten oder elektronische Geräte in der Intensivmedizin. Diese drei Beispiele zeigen die Notwendigkeit auf, daß solche Systeme auch korrekt arbeiten müssen/sollen. Jedoch ist der Nachweis der Funktionstüchtigkeit, die Systemvalidierung, keine einfache Aufgabe. Sie ist unter Umständen gar nicht möglich. Es ist z. B. aus der Komplexitätstheorie bekannt, daß es keinen Algorithmus (also kein vollautomatisches Verfahren) geben kann, daß entscheidet, ob ein beliebiges Computer Programm (z. B. in C oder JAVA geschrieben) terminiert, oder nicht.

Die am meisten genutzten Techniken sind Testen und Simulation. Die Simulation wird an einem abstrakten Modell des Systems durchgeführt, getestet wird dann das eigentliche Endprodukt. Bei einem Computerchip könnte das Testen z. B. so aussehen, daß man an gewissen Stellen des fertigen Chips ein Signal anlegt und die resultierenden Signale an anderen Punkten des Chips abliest und mit den gewünschten Ergebnissen vergleicht. Falls der Chip z. B. 50 Eingabepins besitzt, so hätte man also 2^{50} verschiedene mögliche Eingabebelegungen zu testen. Man sieht also, daß es praktisch unmöglich ist, alle Belegungen zu testen. Deswegen können durch Simulation und Testen zwar Fehler entdeckt werden, aber nicht die Fehlerfreiheit eines Systems garantiert werden.

Eine Möglichkeit, ein gegebenes System zu validieren, ist, durch deduktives Argumentieren die gewünschten Eigenschaften des Systems nachzuweisen. Dies wurde früher von hand gemacht. Da die Systeme immer komplexer und größer werden, ist dies heute fast nicht mehr möglich. Es gibt zwar Programme, die einem dabei helfen, jedoch fordern diese eine gewisse Vorbildung des Benutzers und die

Validierung ist sehr zeitintensiv.

Es wäre also schön, wenn es vollautomatische Verfahren gäbe, die gewisse Eigenschaften von Systemen nachweisen könnten. Anfang der 80er Jahre wurde das sogenannte *Model Checking* entwickelt (siehe [ClEm81]), das genau dieses kann, d. h. gegenüber den anderen Verfahren folgende Vorteile hat:

- Im Gegensatz zu Testen und Simulation kann Model Checking die Fehlerfreiheit eines Systementwurfs garantieren.
- Bei einem System, das die gewünschten Anforderungen nicht erfüllt, gibt Model Checking dem Benutzer einen Fehlerhinweis.
- Verglichen mit den manuellen und halbautomatischen Verifikationssmethoden ist Model Checking sehr effizient und kostengünstig und erfordert keinen fachkundigen Benutzer.

Beim Model Checking wurden früher die gegebenen Systeme durch gerichtete Graphen dargestellt, in denen die Knoten mit gewissen Eigenschaften markiert sind. Die Knoten des Graphen repräsentieren die verschiedenen Zustände, in denen sich das System befinden kann, und die Kanten stehen für die möglichen Übergänge zwischen zwei Zuständen. Die zu überprüfende Eigenschaft wird als Formel einer temporalen Logik dargestellt. Es gibt verschiedene solcher temporalen Logiken, mit denen man unterschiedliche Eigenschaften formulieren kann. Für die Industrie blieb Model Checking jedoch einige Jahre uninteressant, weil industrielle Systeme zu groß waren, um mit herkömmlichen Model Checking Tools behandelt zu werden. Dies änderte sich jedoch, als Ken McMillan Ende der 80er Jahre Systeme mit Hilfe von Binären Entscheidungsgraphen symbolisch darstellte (siehe [McMi93]). Es wurde dann schnell möglich, Systeme mit bis zu 10^{20} Zuständen darstellen und Model Checking mit diesen zu betreiben (siehe [BCM+92]). Bis heute wurden diese Techniken immer weiter verbessert und erweitert, so daß es heute möglich ist, Systeme bis zu 10^{120} Zuständen behandeln zu können. Mc Millan entwickelte als Teil seiner Dissertation den symbolischen Model Checker *SMV*, welcher seitdem immer weiter entwickelt und verbessert wurde. Mit *SMV* konnte z. B. im Nachhinein der Anfang der 90er Jahre berühmt gewordene Fehler im INTEL Pentium Dividierer nachgewiesen werden. Dieser Hardware Fehler hatte einen finanziellen Verlust von rund 475 Mio US Dollar zur Folge.

Heutzutage ist es sogar in gewissen Fällen möglich, unendlich große Systeme zu model checken. Dies erreicht man z. B. , indem man das gegebene System

durch eine geeignete Äquivalenzrelation teilt, so daß die gewünschten Eigenschaften erhalten bleiben.

Probleme ganz anderer Art stellen sich bei Probabilistischen Systemen. Diese kommen z. B. in der Kommunikationstechnik vor. Man stelle sich ein einfaches Sender/Empfänger Modell vor, bei dem der Nachrichtenaustausch über ein nicht sicheres Medium verläuft, d. h. , eine gesendete Nachricht geht mit einer positiven Wahrscheinlichkeit verloren. Auch hier wurden Model Checking Algorithmen entwickelt, die es ermöglichen, Anforderungen wie

"Mit W'keit 1 erfüllt ein gegebenes System eine gewisse Eigenschaft"

zu überprüfen.

Weitaus bedeutsamer sind jedoch quantitative Analysen, die es z. B. ermöglichen, die Wahrscheinlichkeit für das Auftreten eines Ereignisses zu berechnen. Insbesondere können also Anforderungen der Art

"Mit W'keit $> p$ erfüllt ein gegebenes System eine gewisse Eigenschaft",

überprüft werden ($p \in [0,1]$).
Diese Eigenschaften werden in der sogenannten *Linear Time Logik* formuliert. Wir werden im Verlauf dieser Arbeit zwei Model Checking Algorithmen für obige Problemstellung herausarbeiten und auch deren Zeitkomplexität betrachten. Als Grundlage dafür dienen uns die Artikel [CoYa88] und [CoYa95]. Es ist hier noch zu erwähnen, daß das hier behandelte Problem *PSPACE* hart ist (siehe [Va85]).

1.1 Verifikationsmethoden

1.1.1 Transitionssysteme

Es gibt mehrere Modelle zur Beschreibung von formalen Systemen. Eines der Standardmodelle sind *Transitionssysteme*, mit denen sich sowohl Hardwaresysteme als auch Softwaresysteme (Programme) verifizieren lassen. Wie wir gleich sehen werden, sind Transitionssysteme markierte gerichtete Graphen, deren Knoten die verschiedenen Zustände unseres Systems repräsentieren. Im Fall von Softwaresystemen können diese z.B. für die verschiedenen Belegungen von Kontroll- und Programmvariablen stehen. Bei Hardwaresystemen repräsentieren die Knoten die Belegungen der Register und der Ein- und Ausgabebits. Die Kanten stehen für mögliche Zustandswechsel unseres Systems. Zusätzlich werden die Knoten mit sogenannten atomaren Aussagen markiert, die zur Formalisierung temporaler Eigenschaften benötigt werden.

Formale Definition

Definition 1.1.1. [Transitionssystem (TS)]
Ein Transitionssystem ist ein Tupel

$$\mathcal{T} = (S, \rightarrow, S_0, AP, L)$$

bestehend aus

- einer Menge S von Zuständen,
- einer Menge $S_0 \subseteq S$ von Anfangszuständen,
- einer Menge AP von atomaren Aussagen,
- einer Markierungsfunktion $L : S \rightarrow 2^{AP}$,
- einer Transitionsrelation

  $$\rightarrow \subseteq S \times S,$$

  wobei wir $s \longrightarrow s'$ statt $(s, s') \in \rightarrow$ schreiben.

$\mathcal{T}$ heißt *endlich*, falls S und AP endlich sind. ■

Die Markierungsfunktion assoziiert mit jedem Zustand die atomaren Aussagen, die in diesem Zustand wahr sind. In der Literatur, siehe z. B. [CGP00], wird auf Transitionssysteme oft als *Kripke-Strukturen* hingewiesen.

Bemerkung 1. Häufig sind in einem Transitionssystem auch die Kanten mit verschiedenen Aktionen markiert. Da wir hier keinen Gebrauch von Aktionen machen, wurden diese weggelassen.

Nun folgen noch einige weitere Definitionen.

Definition 1.1.2. [Nachfolgermengen]
Sei $\mathcal{T} = (S, \rightarrow, S_0, AP, L)$ ein Transitionssystem und $s \in S$. Wir definieren:

$$Post(s) \quad = \quad \left\{ s' \in S \ : \ s \longrightarrow s' \right\} \ .$$

Jeder Zustand $s' \in Post(s)$ wird unmittelbarer Nachfolger von s genannt.

Definition 1.1.3. [Terminale Zustände]
Sei $\mathcal{T} = (S, \rightarrow, S_0, AP, L)$ ein Transitionssystem und $s \in S$. s heißt *terminal*, wenn $Post(s) = \emptyset$, wenn also in $\mathcal{T}$ keine Kanten von s ausgehen.

Bemerkung 2. [**Transitionssysteme ohne terminale Zustände]** Wir werden im folgenden nur (endliche) Transitionssysteme ohne terminale Zustände betrachten. Dies stellt keine Einschränkung dar, wie folgende Überlegung zeigt.
Sei $\mathcal{T} = (S, \rightarrow, S_0, AP, L)$ ein endliches Transitionssystem. Nun fügen wir für jeden terminalen Zustand $s \in S$ einen Zustand s_{stop} und die Transitionen $s \rightarrow s_{stop}$ und $s_{stop} \rightarrow s_{stop}$ hinzu.

Definition 1.1.4. [Pfadfragmente, Pfade]
Sei $\mathcal{T}$ wie oben und $s \in S$. Ein *Pfadfragment* in $\mathcal{T}$ ist eine unendliche Zustandsfolge

$$\pi \ = \ s_0, s_1, s_2, \ldots$$

so daß $s_i \in \mathit{Post}(s_{i-1}),\ \ i = 1, 2, \ldots$. Die Menge aller in s beginnenden Pfadfragmente wird mit $\mathit{Paths}(s)$ bezeichnet.
Ein Pfadfragment heißt *initial*, falls der erste Zustand s_0 ein Anfangszustand von $\mathcal{T}$ ist. Ein initiales Pfadfragment wird *Pfad* genannt. Mit $\mathit{Paths}(\mathcal{T})$ bezeichnen wir die Menge aller Pfade in $\mathcal{T}$. ■

Definition 1.1.5. [Spuren (Traces)]
Sei $\mathcal{T} = (S, \rightarrow, S_0, AP, L)$ ein Transitionssystem ohne terminale Zustände. Die Spur (engl. trace) eines Pfadfragments π ist das durch die Markierungsfunktion L induzierte unendliche Wort über dem Alphabet 2^{AP} und wird mit $\mathit{trace}(\pi)$ bezeichnet. Für $\pi = s_0, s_1, \ldots$ ist also

$$\mathit{trace}(\pi) \ = \ L(s_0), L(s_1), \ldots$$

Eine Spur von $\mathcal{T}$ bezeichnet die Spur eines Pfads von $\mathcal{T}$.
Mit $\mathit{Traces}(\mathcal{T})$ bezeichnen wir die Menge aller Spuren in $\mathcal{T}$, also $\mathit{Traces}(\mathcal{T}) = \{\mathit{trace}(\pi) : \pi \text{ ist Pfad von } \mathcal{T}\}$. ■

1.1.2 Die *Linear Time* Sicht

Für Systeme, die für den Endlosbetrieb konzipiert sind (z. B. Betriebssysteme, Fahrkartenautomaten) spielen temporale Eigenschaften der Art " ein gewisser Zustand wird irgendwann erreicht" oder " ein gewisser Zustand wird unendlich oft erreicht" eine grosse Rolle. Um solche Eigenschaften zu beschreiben, benutzt man *temporale Logiken*, die schon im Altertum untersucht wurden. 1977 schlug Amir Pnueli vor, solche Logiken in der Verifikation von abstrakten Systemen einzusetzen (siehe [Pnue77]).
Die hier behandelte temporale Logik ist eine Erweiterung der Aussagenlogik. Sie ermöglicht temporale Aussagen wie

$\Diamond$ “eventually” (irgendwann in der Zukunft)
$\Box$ “always” (jetzt und in allen folgenden Zeitpunkten)

und wird *Linear Time Logik (LTL)* genannt.
LTL ist ein sehr einfacher Formalismus, der dennoch mächtig genug ist, relevante Eigenschaften von realen Systemen zu beschreiben. Aufgrund dieser Eigenschaften wird *LTL* auch in einigen Verifikationstools (z.B. SPIN) benutzt.

Die *LTL* Syntax

Wir folgen der Definition in [CGP00].

Definition 1.1.6. [Syntax von *LTL*]
Sei *AP* eine Menge von atomaren Aussagen.
LTL-Formeln über *AP* werden aus folgender Grammatik gebildet.[1]

$$\varphi ::= true \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid X\varphi \mid \varphi_1 \mathcal{U} \varphi_2$$

wobei $a \in AP$. ■

Hieraus kann man die oben erwähnten Operatoren ableiten :

$$\Diamond\varphi \;=\; true\mathcal{U}\varphi \qquad \Box\varphi \;=\; \neg\Diamond\neg\varphi.$$

Auch die üblichen Operatoren der Aussagenlogik lassen sich hiervon ableiten, z. B. :

$$\varphi_1 \vee \varphi_2 \;=\; \neg(\neg\varphi_1 \wedge \neg\varphi_2) \quad \text{and} \quad \varphi_1 \rightarrow \varphi_2 \;=\; \neg\varphi_1 \;\vee\; \varphi_2.$$

Für eine *LTL*-Formel φ über einer beliebigen Aussagenmenge bezeichnen wir mit

$$|\varphi|$$

die *Länge* von φ, welche die Anzahl an Operatoren in φ angibt.

Bevor wir nun zur formalen *LTL*-Semantik kommen, machen wir uns ein Bild

[1] Bemerke, daß wir Nichtterminale mit den ableitbaren Wörtern (Formeln) indentifizieren und Indizes für diese verwenden. Terminal sind offensichtlich $true$, $a \in AP$, $\wedge$, $\neg$, X, $\mathcal{U}$.

über die “intuitive” Bedeutung der temporalen Operatoren :
$X\varphi$ bedeutet, daß φ im nächsten “Schritt” gelten wird.
$\varphi_1 \mathcal{U} \varphi_2$ bedeutet, daß φ_2 irgendwann in der Zukunft gelten wird und daß φ_1 zuvor kontinuierlich gilt.
Somit erhalten wir folgendes für die “intuitive” Bedeutungen von $\Diamond$ and $\Box$:
$\Diamond\varphi$ bedeutet, daß φ irgendwann in der Zukunft gelten wird, während $\Box\varphi$ bedeutet, daß ab jetzt immer φ gelten wird.

Man kann nun durch Kombination der beiden temporalen Operatoren $\Diamond$ und $\Box$ zwei weitere wichtige Operatoren erhalten :

$\Box\Diamond\varphi$ “unendlich oft φ”
$\Diamond\Box\varphi$ “schließlich für immer φ”

Um dies zu vertiefen, folgen zwei einfache Beispiele :

Beispiel 1.1.1. [*LTL*-Formeln]

- Gegeben sei ein System mit zwei Prozessen **A** und **B** mit kritischen Abschnitten $crit_A$ und $crit_B$. Es darf niemals vorkommen, daß sich beide Prozesse gleichzeitig in ihren kritischen Abschnitten befinden. Man kann nun die Zustände des Systems, in denen sich Prozess **A** in Abschnitt $crit_A$ befindet mit $crit_A$ markieren. Das entsprechende macht man mit Zuständen, in denen sich Prozess **B** in Abschnitt $crit_B$ befindet. Nun kann man die geforderte Bedingung des gegenseitigen Ausschlusses mit folgender *LTL*-Formel φ formalisieren.
$$\varphi = \Box(\neg crit_A \vee \neg crit_B)$$
Diese sichert zu, daß sich immer($\Box$) mindestens einer der beiden Prozesse nicht in seinem kritischen Abschnitt befindet.

- Wenn wir sicherstellen wollen, daß sich beide beide Prozesse unendlich oft in ihrem kritischen Abschnitt befinden, so können wir diese Anforderung durch die *LTL*-Formel
$$\varphi = (\Box\Diamond crit_A) \wedge (\Box\Diamond crit_B)$$
beschreiben.

Solche Anforderungen hat man z. B. bei einem Ampelsystem. Man muss dort sicherstellen, daß zwei “komplementäre” Ampeln nie gleichzeitig grün sind und auch, daß jede Ampel nicht für immer die Grünphase vermeidet.

$$
\begin{array}{lcll}
\sigma & \models & \mathit{true} & \\
\sigma & \models & a & \text{gdw} \quad a \in A_0 \\
\sigma & \models & \varphi_1 \wedge \varphi_2 & \text{gdw} \quad \sigma \models \varphi_1 \text{ und } \sigma \models \varphi_2 \\
\sigma & \models & \neg\varphi & \text{gdw} \quad \sigma \not\models \varphi \\
\sigma & \models & X\varphi & \text{gdw} \quad \mathit{suffix}(\sigma,1) = A_1, A_2, A_3, \ldots \models \varphi \\
\sigma & \models & \varphi_1 \mathcal{U} \varphi_2 & \text{gdw} \quad \exists j \geq 0 \,[\, \mathit{suffix}(\sigma,j) \models \varphi_2 \text{ und} \\
 & & & \quad\;\; \mathit{suffix}(\sigma,i) \models \varphi_1,\ i = 0,1,\ldots,j-1 \,]
\end{array}
$$

Abbildung 1.1: *LTL*-Semantik für unendliche Wörter über 2^{AP}

Die *LTL* Semantik

Intuitiv beschreiben *LTL*-Formeln Eigenschaften, die ein Pfadfragment eines Transitionssystems (resp. dessen Spur) haben kann oder nicht. Um in der Lage zu sein, präzise sagen zu können, wann ein Pfad eine gegebene *LTL*-Formel φ erfüllt, definieren wir die Semantik von φ zuerst als eine Sprache $\mathit{Words}(\varphi)$ unendlicher Wörter über dem Alphabet 2^{AP}.
Wir können dann diese Semantik wie folgt dahingehend erweitern, daß man sie über Pfadfragmenten eines Transitionssystems interpretieren kann : Ein Pfadfragment π erfüllt φ genau dann, wenn dessen Spur $\mathit{trace}(\pi)$ in $\mathit{Words}(\varphi)$ enthalten ist.

Definition 1.1.7. [Semantik von *LTL* (Interpretation über unendl. Wörter)]
Sei φ eine *LTL*-Formel über *AP*. Wir definieren

$$\mathit{Words}(\varphi) \;=\; \left\{\sigma \in \left(2^{AP}\right)^{\infty} : \sigma \models \varphi\right\}$$

wobei

$$\models \;\subseteq\; \left(2^{AP}\right)^{\infty} \times \mathit{LTL}$$

die kleinste Relation ist, die die in Abbildung 1.1 angegebenen Eigenschaften besitzt. Wir nennen $\models$ die Erfülltrelation. Dabei ist für $\sigma = A_0, A_1, A_2, \cdots \in \left(2^{AP}\right)^{\infty}$ $\mathit{suffix}(\sigma, j) = A_j, A_{j+1}, A_{j+2}, \ldots$. ■

Somit erhalten wir folgendes für die abgeleiteten Operatoren $\Diamond$ und $\Box$:

$$\begin{array}{lcll} \sigma & \models & \Diamond\varphi & \text{gdw} \quad \exists j \geq 0 \; [\, \mathit{suffix}(\sigma, j) \models \varphi \,] \\ \sigma & \models & \Box\varphi & \text{gdw} \quad \forall j \geq 0 \; [\, \mathit{suffix}(\sigma, j) \models \varphi \,] \end{array}$$

Die durch Kombination erhaltenen Operatoren $\Diamond\Box$ und $\Box\Diamond$ erhalten mit der formalen Semantik ihre "intuitive" Bedeutung "schließlich für immer" und "unendlich oft" :

$$\begin{array}{lcll} \sigma & \models & \Box\Diamond\varphi & \text{gdw} \quad \overset{\infty}{\exists}\, j \; [\, \mathit{suffix}(\sigma, j) \models \varphi \,] \\ \sigma & \models & \Diamond\Box\varphi & \text{gdw} \quad \overset{\infty}{\forall}\, j \; [\, \mathit{suffix}(\sigma, j) \models \varphi \,] \end{array}$$

$\overset{\infty}{\exists}$ steht für "es gibt unendlich viele"
und $\overset{\infty}{\forall}$ steht für "fast alle" (alle, bis auf endlich viele).

Aufbauend auf diesem Formalismus können wir nun die Erfülltrelation $\models$ auf Pfadfragmente und Zustände eines Transitionssystems $\mathcal{T}$ erweitern. Wir sagen ein Pfadfragment π erfüllt eine Formel φ, wenn dessen Spur in $\mathit{Words}(\varphi)$ ist. Ein Zustand s erfüllt φ, wenn alle von ihm ausgehenden Pfadfragmente φ erfüllen. Das ganze Transitionssystem $\mathcal{T}$ erfüllt φ, wenn alle seine Pfade (initiale Pfadfragmente) φ erfüllen.
Das führt uns zu folgender Definition.

Definition 1.1.8. [**Semantik von** *LTL* **(Interpretation über Pfadfragmente und Zustände)]**
Sei $\mathcal{T} = (S, \mathit{Act}, \rightarrow, S_0, \mathit{AP}, L)$ ein Transitionssystem ohne terminale Zustände und φ eine *LTL*-Formel über *AP*. Ein Pfadfragment π von $\mathcal{T}$ erfüllt φ ($\pi \models_{\mathcal{T}} \varphi$), wenn $\mathit{trace}(\pi)$ die Formel φ erfüllt ($\mathit{trace}(\pi) \in \mathit{Words}(\varphi)$). Also

$$\pi \models \varphi \quad \text{gdw} \quad \mathit{trace}(\pi) \models \varphi.$$

Ein Zustand s von $\mathcal{T}$ erfüllt φ, wenn alle in ihm beginnenden Pfadfragmente π die Formel φ erfüllen. Somit :

$$s \models \varphi \quad \text{gdw} \quad \forall \pi \in \mathit{Paths}(s) \;\; [\;\; \pi \models \varphi \;\;]$$

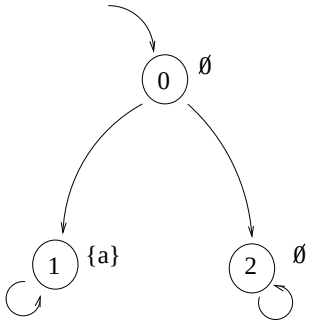
Wir sagen daß $\mathcal{T}$ die Formel φ erfüllt ($\mathcal{T} \models \varphi$), wenn $\mathit{Traces}(\mathcal{T}) \subseteq \mathit{Words}(\varphi)$. ■

Somit gelten offenbar folgende Äquivalenzen :

$$\begin{array}{ll} & \mathcal{T} \models \varphi, \text{ i.e. } \mathit{Traces}(\mathcal{T}) \subseteq \mathit{Words}(\varphi) \\ \text{gdw} & \pi \models \varphi \text{ for all } \pi \in \mathit{Paths}(\mathcal{T}) \\ \text{gdw} & s_0 \models \varphi \text{ for all } s_0 \in S_0. \end{array}$$

Zur Vertiefung dieser Sachverhalte folgt nun ein kleines Beispiel.

Beispiel 1.1.2. Wir betrachten folgendes Transitionssystem $\mathcal{T}$ mit der Zustandsmenge $S = \{0,1,2\}$, der Menge $S_0 = \{0\}$ von Anfangszuständen und der Menge $AP = \{a\}$ von atomaren Aussagen. Bei einer graphischen Darstellung ist es üblich, die Anfangszustände, hier nur 0, durch einen eingehenden Pfeil zu kennzeichnen. Die Markierungsfunktion wird dargestellt, indem neben jeden Zustand seine Markierung geschrieben wird. Die Transitionsrelation wird durch gerichtete Kanten zwischen den Zuständen visualisiert.



Offensichtlich hat $\mathcal{T}$ nur zwei verschiedene Pfade, nämlich $\pi_1 = 0,1,1,\ldots$ und $\pi_2 = 0,2,2,\ldots$ mit den korrespondierenden Spuren $\mathit{trace}(\pi_1) = \emptyset,\{a\},\{a\},\ldots$ und $\mathit{trace}(\pi_2) = \emptyset,\emptyset,\emptyset,\ldots$. Für die *LTL*-Formel $\varphi_1 = \Diamond a \vee XX\neg a$ gilt $\mathit{trace}(\pi_1) \models \varphi_1$ und $\mathit{trace}(\pi_2) \models \varphi_1$.
Da π_1 und π_2 die einzigen Pfade von $\mathcal{T}$ sind, folgt

$$\mathcal{T} \models \varphi_1.$$

Sei $\varphi_2 = \Diamond a$. Beachte, daß gilt : $\mathcal{T} \not\models \varphi_2$ und $\mathcal{T} \not\models \neg\varphi_2$, da

$$\mathit{trace}(\pi_1) = \emptyset,\{a\},\{a\},\{a\},\ldots \models \varphi_2 \text{ und } \mathit{trace}(\pi_2) = \emptyset,\emptyset,\emptyset,\emptyset,\ldots \not\models \varphi_2.$$

Somit sind $\mathcal{T} \not\models \varphi$ und $\mathcal{T} \models \neg\varphi$ nicht äquivalent.

Dies soll nun erstmal als Einführung in die Modellierung von Systemen und die Formalisierung gewisser temporaler Eigenschaften genügen. Wie man dann in der Praxis prüft, ob ein gegebenes Transitionssystem eine *LTL*-Formel erfüllt, werden wir in Abschnitt 2.2.1 auf Seite 32 sehen.

Als nächstes wenden wir uns der Modellierung von Probabilistischen Systemen zu.

1.2 Probabilistische Systeme

Wie wir im vorigen Abschnitt gesehen haben, lassen sich viele reale Systeme, wie z.B. Ampelschaltungen mit Transitionssystemen modellieren. Zusätzlich lassen sich auch noch temporale Eigenschaften wie z.B. "Ampel A und Ampel B dürfen niemals gleichzeitig grün" sein in *LTL*-Formeln ausdrücken. Es läßt sich dann, wie wir später noch sehen werden, überprüfen, ob unser Modell die gewünschte Eigenschaft besitzt. Nun tauchen aber in der Praxis oft gewisse Unsicherheitsfaktoren auf. Es kann z.B. bei Kommunikationsvorgängen vorkommen, daß das Transportmedium keine 100%ige Zuverlässigkeit besitzt. Nun wäre es wünschenswert, wenn man, unter der Voraussetzung, daß man die Fehlerraten kennt (bzw. abschätzen kann), solche Situationen auch modellieren könnte und zusätzlich nachprüfen könnte, ob eine Aussage der Art "mit der Wahrscheinlichkeit 0,98 erfüllt mein System eine gegebene *LTL*-Formel" wahr ist. Und genau da greift Probabilistisches Model Checking.

1.2.1 Modellierung probabilistischen Verhaltens

Wir beschränken uns hier auf Systeme mit endlichen Zustandsmengen. Als Grundbaustein unseres Modells dienen uns endliche Markov Ketten.

Endliche Markov Ketten

Definition 1.2.1. [Endliche Markov Kette]
Eine *endliche Markov Kette*

$$M = (X,\ T,\ p,\ p_0)$$

ist ein Tupel bestehend aus

- einer endlichen Menge X von Zuständen,

- einer Menge $T \subseteq X \times X$ von Transitionen,
- einer Zuordnung von *Transitionswahrscheinlichkeiten* $p : T \longrightarrow \mathbb{R}^+$ mit

$$\sum_{v \in X} p((u,v)) = 1 \quad \forall u \in X$$

  Wir werden in Zukunft p_{uv} statt $p((u,v))$ schreiben. Aus technischen Gründen definieren wir

$$p_{uv} = 0 \quad \forall (u,v) \notin T.$$

- einer *initialen Wahrscheinlichkeitsverteilung* $p_0 : X \longrightarrow \mathbb{R}_0^+$, so daß

$$\sum_{u \in X} p_0(u) = 1.$$

■

Man kann sich eine Markov Kette als gerichteten Graphen vorstellen, dessen Kanten stochastisch gewichtet sind. Zusätzlich besitzt dieser Graph noch eine initiale Wahrscheinlichkeitsverteilung auf seinen Knoten. (X,T) heißt der *zugrundeliegende Graph* von M.

Definition 1.2.2. [Erweiterung von p auf endliche Folgen von Zuständen]
Sei $y = x_0, x_1, \ldots, x_n$ eine endliche Folge von Zuständen von M. Dann definieren wir $p_y = p_0(x_0) \cdot p_{x_0 x_1} \cdot p_{x_1 x_2} \cdots p_{x_{n-1} x_n}$. ■

Bemerke, daß eine Markov Kette keine terminalen Zustände besitzen kann, da in jedem Zustand die Summe der Wahrscheinlichkeiten der ausgehenden Transitionen gleich 1 sein muß.

Definition 1.2.3. [Lauf einer Markov Kette]
Als *Lauf* $Y = x_0, x_1, x_2, \ldots$ einer Markov Kette definieren wir eine unendliche Folge von Zuständen der Markov Kette. ■

Definition 1.2.4. [Echter Lauf einer Markov Kette]
Als *echten Lauf* $Y = x_0, x_1, x_2, \ldots$ einer Markov Kette definieren wir eine unendliche Folge von Zuständen der Markov Kette, für die gilt:

$$p_0(x_0) > 0 \quad \wedge \quad p_{x_{i-1} x_i} > 0 \quad \forall i \in \mathbb{N},$$

also $(x_{i-1}, x_i) \in T \quad \forall i \in \mathbb{N}$. Ein echter Lauf einer Markov Kette ist also ein unendlicher Pfad in deren zugrundeliegendem Graphen mit von Null verschiedener Anfangswahrscheinlichkeit. ■

Eine Markov Kette M induziert nun auf natürliche Weise einen stochastischen Prozeß auf der Menge der Zustände von M. Die Wahrscheinlichkeitsverteilung in Schritt $n = 0$ entspricht p_0. Ausserdem gilt, daß die Wahrscheinlichkeitsverteilung in Schritt $n \geq 1$ gegeben die Schritte $0, 1, \ldots, (n-1)$ nur vom letzten Schritt $(n-1)$ abhängt und gleich den Transitionswahrscheinlichkeiten ist. Das bedeutet, daß für alle $u, v \in X$ gilt : gegeben, daß u in Schritt $(n-1)$ erreicht wurde, ist die Wahrscheinlichkeit dafür, daß v in Schritt n erreicht wurde, gleich p_{uv}. Dies bezeichnet man als sogenannte *Markov-Eigenschaft*, auf die wir noch häufiger verweisen werden. Für diesen Prozeß kann man nun einen Wahrscheinlichkeitsraum angeben.

Definition 1.2.5. [**Basiszylinder über X**]
Gegeben sei eine endliche Markov Kette M wie oben.
$\forall n \in \mathbb{N},\ \forall x_0, x_1, \ldots, x_n \in X$ heißt

$$\Delta(x_0, x_1, \ldots, x_n) = \{y_0, y_1, \ldots \in X^\omega \mid y_i = x_i \ \ \forall i \in \{0, 1, 2, \ldots, n\}\}$$

ein Basiszylinder über X.
$\Delta(x_0, x_1, \ldots, x_n)$ ist also die Menge aller Läufe von M, für die $x_0, x_1, \ldots, x_n$ ein Präfix ist. Wir nennen n die *Länge* des Basiszylinders $\Delta(x_0, x_1, \ldots, x_n)$. ■

Bemerke, daß $\Delta(x)$ gerade die Menge der in x beginnenden Läufe ist.

Definition 1.2.6. [**Der Folgenraum einer endlichen Markov Kette**]
Gegeben sei eine endliche Markov Kette $M = (X,\ T,\ p,\ p_0)$.
Als *Folgenraum* von M definieren wir den Wahrscheinlichkeitsraum

$$\Psi_M = (X^\omega, \Delta, \mu),$$

wobei

- Δ die von allen *Basiszylindern* über X, X^ω und der leeren Menge erzeugte σ-Algebra ist
- μ das eindeutig[2] bestimmte Wahrscheinlichkeitsmaß ist, das folgende Eigenschaft erfüllt : $\forall$ Basiszylinder über X gilt

$$\mu(\Delta(x_0, x_1, \ldots, x_n)) = p_0(x_0)\, p_{x_0 x_1} \cdots p_{x_{n-1} x_n}$$

[2] wegen Schnittstabilität der Basiszylinder (siehe [Bau78])

■

An dieser Definition läßt sich leicht die Markov-Eigenschaft erkennen.
Wer mehr über stochastische Prozesse und Markov Ketten wissen will, sei auf [KS60] und [KSK76] hingewiesen. Für Erläuterungen zu Wahrscheinlichkeitstheorie, siehe z. B. [Bau78].

Bemerkung 3. [**{Läufe in M} \ {echte Läufe in M} hat Maß** 0 **]**
Sei $\Upsilon = \{Y \mid Y \text{ Lauf in } M\} \setminus \{Y \mid Y \text{ echter Lauf in } M\}$. Dann ist Υ die abzählbare Vereinigung von Basiszylindern der Art $\Delta(x_0, x_1, \ldots, x_n)$ mit $(x_{i-1}, x_i) \in T, 1 \leq i \leq (n-1)$ und $(x_{n-1}, x_n) \notin T$ oder $p_0(x_0) = 0$. Jeder solche Basiszylinder hat Maß 0 und somit gilt $\mu(\Upsilon) = 0$.

Probabilistisches Programm

Wie schon erwähnt, bilden die Markov Ketten den Grundbaustein unseres Modells zur Modellierung probabilistischen Verhaltens. Um in unserem System gewisse Eigenschaften darstellen zu können, werden wir wie bei Transitionssystemen die Zustände der Markov Kette markieren.

Definition 1.2.7. [**Probabilistisches Programm]**
Ein Probabilistisches Programm ist ein Tupel

$$\mathcal{T}_{prob} = (M, AP, L) \ ,$$

wobei

- $M = (X,\ T,\ p,\ p_0)$ eine endliche Markov Kette ist,
- AP eine Menge von atomaren Aussagen ist und
- $L : X \to 2^{AP}$ eine Markierungsfunktion ist.

■

Ein Probabilistisches Programm ist also nichts anderes als ein Transitionssystem, bei dem die Transitionen und Anfangszustände mit Wahrscheinlichkeiten versehen sind. Somit können wir die bereits vorbereitete Theorie der Transitionssysteme auf Probabilistische Programme übertragen.

Definition 1.2.8. [**Lauf eines Probabilistischen Programms]**
Sei $\mathcal{T}_{prob} = (M, AP, L)$ ein Probabilistisches Programm. Ein Lauf Y der Markov Kette M wird zugleich auch Lauf von $\mathcal{T}_{prob}$ genannt. ■

Definition 1.2.9. [**Spur eines Probabilistischen Programms]**
Sei $\mathcal{T}_{prob} = (M, AP, L)$ ein Probabilistisches Programm und $Y = x_0, x_1, \ldots$ ein Lauf von $\mathcal{T}_{prob}$. Dann bezeichnen wir mit

$$trace(Y) \;=\; L(x_0), L(x_1), \ldots$$

die Spur von Y. Eine Spur von $\mathcal{T}_{prob}$ bezeichnet die Spur eines Laufs von $\mathcal{T}_{prob}$. Mit $Traces(\mathcal{T}_{prob})$ bezeichnen wir die Menge aller Spuren in $\mathcal{T}_{prob}$. ■

1.2.2 Probabilistische *Linear Time Logik*

Auch der *LTL*-Formalismus läßt sich nun auf natürliche Weise auf Probabilistische Programme erweitern.

Definition 1.2.10. [**Semantik von** *LTL* **(Interpretation über Läufe)]**
Sei $\mathcal{T}_{prob} = (M, AP, L)$ ein Probabilistisches Programm und φ eine *LTL*-Formel über *AP*.
Wir sagen ein Lauf Y erfüllt φ genau dann, wenn seine Spur φ erfüllt.

$$Y \models \varphi \;\Leftrightarrow\; trace(Y) \models \varphi \;\Leftrightarrow\; trace(Y) \in Words(\varphi).$$

■

Bemerke, daß man beim probabilistischen *LTL*-Model Checking nicht daran interessiert ist, ob alle, von einem Zustand ausgehenden Läufe, eine gegebene *LTL*-Formel φ erfüllen. Stattdessen ist man am Wahrscheinlichkeitsmaß der von diesem Zustand ausgehenden und φ erfüllenden Läufe interessiert. Dies setzt voraus, daß eine solche Menge überhaupt meßbar ist. Dieses Resultat werden wir in 1.3.1 auf Seite 20 beweisen.

Definition 1.2.11. [**Die Mengen** $Y_{\models\varphi}$ **und** $Y_{\not\models\varphi}$**]**
Wir bezeichnen mit $\mathbf{Y}_{\models\varphi}$, bzw. $\mathbf{Y}_{\not\models\varphi}$ die Menge aller Läufe Y in M, die φ erfüllen, bzw. nicht erfüllen. ■

Satz 1.1. *Sei $\mathcal{T}_{prob} = (M, AP, L)$ ein Probabilistisches Programm und φ eine LTL-Formel über AP. Dann ist $\mathbf{Y}_{\models\varphi}$ meßbar in Ψ_M.*
Beweis : siehe 1.3.1 auf Seite 20

Bemerke, daß $\mu(\mathbf{Y}_{\models\varphi})$ gerade die Wahrscheinlichkeit angibt, daß ein Lauf Y von M die Formel φ erfüllt.

Definition 1.2.12. [**Erfülltrelation für Probabilistische Programme]**
Sei $\mathcal{T}_{prob} = (M, AP, L)$ ein Probabilistisches Programm und φ eine *LTL*-Formel über *AP*. Wir sagen, daß $\mathcal{T}_{prob}$ die Formel φ erfüllt, i. Z. : $\mathcal{T}_{prob} \models \varphi$, falls gilt :

$$\mu(\mathbf{Y}_{\models\varphi}) = 1.$$

D. h. , die φ nicht erfüllenden Läufe von *M* bilden eine Nullmenge im Folgenraum Ψ_M von *M*. ■

Bemerkung 4. Gegeben sei ein Probabilistisches Programm $\mathcal{T}_{prob} = (M, AP, L)$ und eine *LTL*-Formel φ. Sei *x* ein Zustand von $\mathcal{T}_{prob}$ mit intialer Wahrscheinlichkeit gleich 0 $(p_0(x) = 0)$. Sei *B* eine in Ψ_M meßbare Menge von in *x* beginnenden Läufen. Dann gilt

$$\mu(B) = 0.$$

Insbesondere ist $\mu(\{Y = x, x_1, x_2, \ldots | Y \text{ Lauf in } M \text{ und } Y \models \varphi.\}) = 0$.
Wenn wir also im folgenden wie oben davon reden, daß wir am Wahrscheinlichkeitsmaß der von einem beliebigen Zustand ausgehenden und φ erfüllenden Läufe interessiert sind, so meinen wir folgendes :
Gegeben sei ein Probabilistisches Programm $\mathcal{T}_{prob} = (M, AP, L)$ und eine *LTL*-Formel φ. Sei *z* ein Zustand von $\mathcal{T}_{prob}$.
Wenn $M = (X,\ T,\ p,\ p_0)$, so definieren wir
$M^z = (X,\ T,\ p,\ p_0^z)$, wobei $p_0^z(z) = 1$ und $p_0^z(x) = 0 \quad \forall x \neq z \in X$. Sei $\Psi_{M^z} = (X^\omega, \Delta, \mu^z)$ der Folgenraum von M^z.[3] Mit dem Wahrscheinlichkeitsmaß der von *z* ausgehenden und φ erfüllenden Läufe bezeichnen wir den Wert

$$\mu^z(\{Y = z, x_1, x_2, \ldots | Y \text{ Lauf in } M^z \text{ und } Y \models \varphi\}) =$$

$$\mu(\frac{\{Y = z, x_1, x_2, \ldots | Y \text{ Lauf in } M \text{ und } Y \models \varphi\}}{p_0(z)}) \text{ , falls } p_0(z) \neq 0.$$

Zur Vertiefung des eben gelesenen werden wir jetzt einige Begriffe an einem Beispiel erläutern.

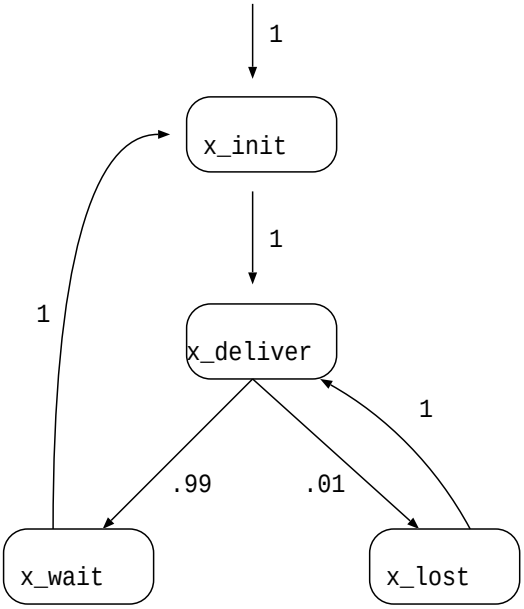
Beispiel 1.2.1. Anlehnend an Kommunikationsprotokolle betrachten wir einen vereinfachten Sender. Dieser generiert eine Nachricht und gibt diese an das Transportmedium weiter, welches die Nachricht an den Empfänger weiterleiten soll. Da nun das Medium nicht 100%ig störungsfrei ist, geht die Nachricht mit Wahrscheinlichkeit 0.01 verloren und wird mit Wahrscheinlichkeit 0.99 korrekt übermittelt. Im letzten Fall wartet der Sender auf die Bestätigung des Empfängers

[3] bemerke, $W \subset X$ ist meßbar in Ψ_M gdw W ist meßbar in Ψ_{M^z}

und kehrt dann zum Anfangszustand zurück. Bemerke, daß diese Bestätigung aus Gründen der Vereinfachung in unserem Beispiel nicht verlorengehen kann. Als Markierungsfunktion sollen in unserem Beispiel die Zustandsnamen stehen. Es gibt die folgenden vier Zustände:

- x_{init}: der Zustand, in dem der Sender die Nachricht generiert und sie an das Medium weiterleitet
- $x_{deliver}$: der Zustand, in dem das Medium versucht, die Nachricht zu senden
- x_{lost}: wird erreicht, wenn die Nachricht verloren ging
- x_{wait}: wird erreicht, wenn die Nachricht erfolgreich gesendet wurde. Hier wartet der Sender dann auf die Bestätigung des Empängers.

Wir erhalten dann folgendes Probabilistische Programm:



Der Wahrscheinlichkeitwert für die endliche Folge $x_{init}, x_{deliver}, x_{lost}, x_{deliver}, x_{wait}$ ist gleich $1 \times 1 \times 0.01 \times 1 \times 0.99 = 0.0099$.
Weiterhin gilt $\mu(\mathbf{Y}_{\models \Diamond x_{wait}}) = 1$, da

$$\mathbf{Y}_{\not\models \Diamond x_{wait}} = \mathbf{Y}_{\models \Box \neg x_{wait}} = \{x_{init}, x_{deliver}, x_{lost}, x_{deliver}, x_{lost}, x_{deliver}, \ldots\} \cup Rest,$$

wobei *Rest* eine meßbare Teilmenge der nicht echten Läufe ist und somit Maß 0 hat.
Beachte, daß sogar gilt: $\mu(\mathbf{Y}_{\models\Box\Diamond x_{wait}}) = 1$. Das kann man leicht sehen, da

$$\mathbf{Y}_{\not\models\Box\Diamond x_{wait}} = \mathbf{Y}_{\models\Diamond\Box\neg x_{wait}} = \cup_{i=0}^{\infty}\mathbf{Y}_{\models X^i\Box\neg x_{wait}}.$$

Aufgrund der Markov Eigenschaft und $\mu(\mathbf{Y}_{\models\Box\neg x_{wait}}) = 0$ folgt $\mu(\mathbf{Y}_{\models X^i\Box\neg x_{wait}}) = 0$. Somit hat $\mathbf{Y}_{\not\models\Box\Diamond x_{wait}}$ als abzählbare Vereinigung von Nullmengen Maß Null und $\mu(\mathbf{Y}_{\models\Box\Diamond x_{wait}}) = \mu(X^\omega \setminus \mathbf{Y}_{\not\models\Box\Diamond x_{wait}}) = 1-0 = 1$.

1.3 über Markov Ketten

1.3.1 Die Sprache einer *LTL*-Formel ist meßbar

Wir werden jetzt den in Definition 1.2.12 benutzten Satz 1.1 beweisen.[4]

Satz : *Sei $\mathcal{T}_{prob} = (M, AP, L)$ ein Probabilistisches Programm und φ eine LTL-Formel über AP. Dann ist $\mathbf{Y}_{\models\varphi}$ meßbar in Ψ_M.*
Beweis : durch strukturelle Induktion über φ

- Induktionsanfang :
  - $\varphi = true$: $\mathbf{Y}_{\models true} = X^\omega$ und ist somit meßbar in Ψ_M.
  - $\varphi = a,\ a \in AP$: $\mathbf{Y}_{\models a} = \cup_{x\in X \text{ mit } a\in L(x)}\Delta(x)$ und ist somit meßbar in Ψ_M.
- Induktionsschritt : seien $\mathbf{Y}_{\models\varphi_1}$ und $\mathbf{Y}_{\models\varphi_2}$ meßbar in Ψ_M
  - $\varphi = \neg\varphi_1$: $\mathbf{Y}_{\models\neg\varphi_1} = \mathbf{Y}_{\not\models\varphi_1} = X^\omega \setminus \mathbf{Y}_{\models\varphi_1}$ und ist somit meßbar in Ψ_M.
  - $\varphi = \varphi_1 \wedge \varphi_2$: $\mathbf{Y}_{\models\varphi_1\wedge\varphi_2} = \mathbf{Y}_{\models\varphi_1} \cap \mathbf{Y}_{\models\varphi_2}$ und ist somit meßbar in Ψ_M.
  - $\varphi = X\varphi_1$: sei $f : X^\omega \to X^\omega$ mit $f(y_0, y_1, y_2, \ldots) = y_1, y_2, \ldots$ eine Abbildung. Dann gilt f ist meßbar, da das Urbild eines jeden Basiszylinder meßbar ist ($f^{-1}(\Delta(x_0,\ldots,x_n)) = \cup_{x\in X}\ \Delta(x, x_0, \ldots, x_n)$). Somit ist $\mathbf{Y}_{\models X\varphi_1} = f^{-1}(\mathbf{Y}_{\models\varphi_1})$ meßbar.
  - $\varphi = \varphi_1 \mathcal{U} \varphi_2$: $\mathbf{Y}_{\models\varphi_1\mathcal{U}\varphi_2} = \cup_{i=0}^{\infty}(\mathbf{Y}_{\models X^i\varphi_2} \cap_{j=0}^{i-1} \mathbf{Y}_{\models X^j\varphi_1})$ und ist somit meßbar in Ψ_M.

[4] für Fragen über Wahrscheinlichkeitstheorie siehe [Bau78]

□

1.3.2 Ergodische Mengen

In diesem Abschnitt wollen wir eine wichtige Eigenschaft von endlichen Markov Ketten beweisen, die wir im weiteren Verlauf dieser Arbeit noch häufig zitieren werden. Dazu zuerst folgende Definitionen.

Definition 1.3.1. [**Starke Zusammenhangskomponente (SCC)]**
Gegeben ein gerichteter Graph $G = (V,E)$. Wir nennen $C \subset V$ eine *starke Zusammenhangskomponente* (engl. strongly connected component) von G, falls gilt:

$$\forall u,v \in G \ : \ \exists \text{ Weg von } u \text{ nach } v \text{ in } C$$

und C ist maximal mit obiger Eigenschaft. ■

Definition 1.3.2. [**Ergodische Menge]**
Gegeben ein gerichteter Graph $G = (V,E)$. Sei $C \subset X$ eine starke Zusammenhangskomponente (SCC) von G. Wir nennen C *ergodische Menge* von G, falls es keine Transitionen in G gibt, die aus C hinausführen, d. h.

$$\forall (u,v) \in E \ : \ u \in C \ \Rightarrow \ v \in C.$$

■

Gegeben eine endliche Markov Kette $M = (X,\ T,\ p,\ p_0)$. Wir nennen $C \subset X$ *ergodische Menge* von M, falls C ergodische Menge des zugrundeliegenden Graphen (X,T) von M ist. Es ist offensichtlich, daß von jedem Zustand im Graphen (X,T) eine ergodische Menge erreichbar ist. Bemerke folgendes: gegeben eine ergodische Menge C und ein echter Lauf $Y = x_0,x_1,\ldots$ von M, so gilt :

$$x_i \in C \ \ \Rightarrow \ \ x_j \in C \ \ \forall j \geq i.$$

Es gilt nun für jeden Lauf von M, daß dieser mit Wahrscheinlichkeit 1 eine ergodische Menge C von M erreicht und jeden Zustand von C unendlich oft durchläuft. Wir werden nun ein allgemeineres Resultat beweisen, von dem sich die eben gemachte Aussage leicht ableiten läßt. Dafür noch folgende Definitionen.

Definition 1.3.3. [**Kantenmarkierung einer endlichen Markov Kette]**
Gegeben eine endliche Markov Kette $M = (X,\ T,\ p,\ p_0)$ und eine nichtleere abzählbare Menge K_M von Markierungen. Wir nennen

$$l : X \times X \ \rightarrow \ 2^{K_M}$$

eine *Kantenmarkierung* von M, falls gilt:

$$l(u,v) = \emptyset \quad \forall (u,v) \notin T.$$

■

Wir sagen $\ell \in K_M$ ist *aktiv* in Zustand $x \in X$, falls es ein $y \in X$ gibt, so daß $\ell \in l(x,y)$, d. h. es gibt eine aus x hinausführende Transition, die mit ℓ markiert ist. Für einen Lauf $Y = x_0, x_1, \ldots$ von M sagen wir, daß ℓ im i - ten Schritt von Y *angenommen* wurde, falls $\ell \in l(x_{i-1}, x_i)$.

Definition 1.3.4. [**Fairness]**
Gegeben eine endliche Markovkette M, eine Menge K_M von Markierungen und eine Markierungsfunktion l. Ein Lauf $Y = x_0, x_1, \ldots$ von M heißt *fair bezüglich* $\ell \in K_M$, falls entweder ℓ nur endlich oft aktiv ist in Y, oder ℓ unendlich oft in Y angenommen wird, d. h.

$$\overset{\infty}{\exists}\, i \ : \ \ell \text{ ist aktiv in Zustand } x_i \implies \overset{\infty}{\exists}\, i \ : \ \ell \text{ wird in Schritt } i \text{ von } Y \text{ angenommen.}$$

Wir nennen Y *fair*, falls Y fair bezüglich jeder Markierung ℓ aus K_M ist.
Für $x \in X$ bezeichnen wir mit $Fair(x)$ die in x beginnenden fairen Läufe von M. $Fair_\ell(x)$ bezeichnet für $\ell \in K_M$ die in x beginnenden Läufe von M, die fair bezüglich ℓ sind. ■

Wir zeigen nun, daß wir für ein Probabilistisches Programm $\mathcal{T}_{prob} = (M, AP, L)$ und für $\ell \in K_M$ eine *LTL*-Formel φ_ℓ über AP angeben können, so daß die Menge $Fair_\ell(x)$ gleich der Menge der φ_ℓ erfüllenden Läufe ist. Somit sind nach Satz 1.1 auf Seite 17 die Mengen $Fair_\ell(x)$ und $Fair(x) = \cap_{\ell \in K_M} Fair_\ell(x)$ meßbar in dem Folgenraum Ψ_M.

Zur Konstruktion dieser Formel φ_ℓ :
Gegeben sei eine endliche Markovkette M, eine Menge K_M von Markierungen und eine Markierungsfunktion l. Für alle $\ell \in K_M$ sei n_ℓ die Anzahl an Transitionen (u,v), mit $\ell \in l((u,v))$. Wir definieren

- $AP = \{\ell_j^{out}, \ell_j^{in} \mid \ell \in K_M \text{ und } 1 \leq j \leq n_\ell\}$

- $L : X \to AP$ wird gemäß folgendem Algorithmus definiert :
  $L(x) = \emptyset \ \ \forall x \in X$
  $zähler_\ell := 1 \ \ \forall \ell \in K_M$
  für alle Transitionen $t = (u,v)$ *in* T *{*
  für alle Markierungen $\ell \in l(t)$ *{*
  $L(u) = L(u) \ \cup \ \{\ell^{out}_{zähler_\ell}\}$
  $L(v) = L(v) \ \cup \ \{\ell^{in}_{zähler_\ell}\}$
  $zähler_\ell = zähler_\ell + 1$
  }
  }

Sei nun $Y = x_0, x_1, \ldots$ ein Lauf in $\mathcal{T}_{prob}$. Dann gelten folgende Äquivalenzen:

- ℓ ist aktiv in $x_i \iff \exists j \ : \ \ell^{out}_j \in L(x_i)$
- ℓ wird im i - ten Schritt von Y angenommen $\iff$
  $\exists j \ : (\ell^{out}_j \in L(x_{i-1}) \ \wedge \ \ell^{in}_j \in L(x_i))$

Wir definieren nun für $\ell \in K_M$ die *LTL*-Formeln $\varphi_{aktiv}(\ell)$ und $\varphi_{angenommen}(\ell)$ über *AP*.

- $\varphi_{aktiv}(\ell) = \vee_{1 \le j \le n_\ell} \ell^{out}_j$
- $\varphi_{angenommen}(\ell) = \vee_{1 \le j \le n_\ell} (\ell^{out}_j \ \wedge \ X\ell^{in}_j)$

Somit erhalten wir mit $\varphi(\ell) = (\Box\Diamond\varphi_{aktiv}(\ell) \ \Rightarrow \ \Box\Diamond\varphi_{angenommen}(\ell))$

- $Fair_\ell(x) = \{Y \mid Y \text{ ist in } x \text{ beginnender Lauf mit } Y \models \varphi(\ell)\}$
  $= \Delta(x) \cap \mathbf{Y}_{\models\varphi(\ell)}$
- $Fair(x) = \cap_{\ell \in K_M} Fair_\ell(x)$
  $= \{Y \mid Y \text{ ist in } x \text{ beginnender Lauf mit } Y \models \wedge_{\ell \in K_M}\varphi(\ell)\}.$
  $= \Delta(x) \cap \mathbf{Y}_{\models \wedge_{\ell \in K_M}\varphi(\ell)}$

Also lassen sich die Mengen $Fair(x)$ und $Fair_\ell(x)$ durch *LTL*-Formeln charakterisieren und sind somit nach Satz 1.1 auf Seite 17 meßbar in Ψ_M. Bemerke, daß wir nur an der Menge $Fair^{echt}(x)$ der fairen echten in x beginnenden Läufe interessiert sind. Es gilt jedoch

$$Fair^{echt}(x) = Fair(x) \setminus \Upsilon \quad [5]$$

[5] zur Definition von Υ siehe Bemerkung 3 auf Seite 16

und somit ist $Fair^{echt}(x)$ meßbar in μ, und da Υ eine Nullmenge in μ ist, gilt

$$\mu(Fair^{echt}(x)) = \mu(Fair(x)).^{6}$$

Satz 1.2. *Sei $M = (X,\ T,\ p,\ p_0)$ eine endliche Markov Kette, K_M eine nichtleere abzählbare Menge von Markierungen und l eine Kantenmarkierung von M. Seien $\mathcal{T}_{prob} = (M, AP, L)$, $\varphi_{aktiv}(\ell)$ und $\varphi_{angenommen}(\ell)$ wie oben definiert und $\Psi_M = (X^\omega, \Delta, \mu)$ der Folgenraum von M. Dann gilt*

$$\mu^x(Fair(x)) = 1 \quad \forall x \in X, \textit{ d. h. } \mu(Fair(x)) = p_0(x).$$

Beweis : Es genügt zu zeigen daß $\mu^x(Fair_\ell(x)) = 1 \quad \forall \ell \in K_M$.[7]
Sei $\ell \in K_M$ fest. Sei $c = \min\{p_{uv} \mid (u,v) \in T\}$ (bemerke, $|T| < \infty$). Sei $y = x_0, x_1, \ldots, x_n$ Präfix eines Laufes in M und Π eine Menge von Läufen in M, die in x_n beginnen. Dann bezeichnen wir mit $y\Pi$ folgende Menge von Läufen

$$\{x_0, x_1, \ldots, x_n, y_1, y_2, \ldots \mid Y = y_0, y_1, \ldots \in \Pi\}.^{8}$$

Für $x \in X$ sei nun Π_x die Menge aller in x beginnenden Läufe von M, für die ℓ unendlich oft aktiv ist, aber nie angenommen wird, also

$$\Pi_x = \{Y \mid Y \text{ in } x \text{ beginnender Lauf mit } Y \models \Box\Diamond\varphi_{aktiv}(\ell) \wedge \Box\neg\varphi_{angenommen}(\ell)\}.$$

Somit ist Π_x meßbar. Die weitere Vorgehensweise ist nun folgende. Wir werden zeigen, daß $\mu^x(\Pi_x) = 0$ für alle $x \in X$. Ferner zeigen wir, daß

$$\Gamma(x) = \{Y \mid Y \text{ ist in } x \text{ beginnender Lauf }\} \setminus Fair_\ell(x)$$

als die abzählbare Vereinigung von Mengen der Form $y\Pi_x$ geschrieben werden kann, wobei $y = x_0, x_1, \ldots, x$ Präfix eines Laufes von M ist. Bemerke, daß auch $y\Pi_x$ meßbar und daß

$$\mu^{x_0}(y\Pi_x) = \frac{p_y}{p_0(x_0)} \cdot \mu^x(\Pi_x) = p_{x_0x_1} \cdot p_{x_1x_2} \cdots p_{x_{n-1}x} \cdot \mu^x(\Pi_x) = 0.$$

Somit folgt $\mu^x(\Gamma(x)) = 0$. Wir erhalten somit $\mu^x(Fair_\ell(x)) = 1$. Nun also zu

$$\mu^x(\Pi_x) = 0 \text{ für alle } x \in X.$$

[6] Rufe nochmals Bemerkung 4 auf Seite 18 ins Gedächtnis.

[7] in einem Wahrscheinlichkeitsraum gilt: $\mu(A_i) = 1 \quad i = 1, 2, \ldots$ impliziert $\mu(\cap_{i=1,2,\ldots} A_i) = 1$ (bemerke, daß K_M abzählbar ist)

[8] Beachte, daß $y_0 = x_n$.

Sei *Aktiv* die Menge der Zustände in X, in denen ℓ aktiv ist, d. h. $Aktiv = \{x \in X \mid \exists j : \ell_j^{out} \in L(x)\}$. Für $x \in X$ sei Ω_x die Menge aller mit x beginnenden endlichen Zustandsfolgen, so daß ℓ im letzten Zustand aktiv ist und sonst noch höchstens im ersten Zustand aktiv ist, aber nicht im ersten Schritt angenommen wird, also

$$\Omega_x = \{x, x_1, x_2, \ldots, x_n \mid x_i \notin Aktiv, 1 \leq i \leq (n-1) \text{ und } x_n \in Aktiv \text{ und } \ell \notin l(x, x_1)\}$$

Wir partitionieren Ω_x nun folgendermassen. Für $a \in Aktiv$ und $x \in X$ sei $\Omega_x^a = \{x, x_1, \ldots, x_n \in \Omega_x \mid x_n = a\}$. Ω_x ist also die disjunkte Vereinigung der Ω_x^a, somit $\Omega_x = \cup_{a \in Aktiv} \Omega_x^a$. Diese Vereinigung ist offensichtlich abzählbar und wir erhalten

$$\sum_{y \in \Omega_x} p_y = \sum_{a \in Aktiv} \sum_{y \in \Omega_x^a} p_y \tag{1.1}$$

Zudem gilt offensichtlich für $x \in X$

$$\Pi_x = \cup_{a \in Aktiv} \cup_{y \in \Omega_x^a} y\Pi_a. \tag{1.2}$$

Auch dies ist eine disjunkte Vereinigung.
Sei $a \in Aktiv$. Dann gibt es ein $x_a \in X$, so daß gilt $\ell \in l(a, x_a)$. Es gilt nun:

$$\sum_{y \in \Omega_a} \frac{p_y}{p_0(a)} \leq \sum_{x \neq x_a} p_{ax} = 1 - p_{ax_a} \leq 1 - c \tag{1.3}$$

Nun können wir durch Induktion über k zeigen, daß $\mu^a(\Pi_a) \leq (1-c)^k \quad \forall a \in Aktiv$. Für den Induktionsanfang $k = 0$ ist nichts zu zeigen. Nehmen wir also für den Induktionsschritt an, die Behauptung sei für k bewiesen, also $\mu^a(\Pi_a) \leq (1-c)^k \quad \forall a \in Aktiv$. Sei $b \in Aktiv$ beliebig. Da 1.2 eine disjunkte und abzählbare Vereinigung ist, folgt

$$\mu^b(\Pi_b) = \sum_{a \in Aktiv} \sum_{y \in \Omega_b^a} \mu^b(y\Pi_a) = \sum_{a \in Aktiv} \sum_{y \in \Omega_b^a} \left(\frac{p_y}{p_0(b)} \cdot \mu^a(\Pi_a)\right).$$

Durch die Induktionsvoraussetzung und 1.1 erhalten wir

$$\mu^b(\Pi_b) \leq (1-c)^k \sum_{a \in Aktiv} \sum_{y \in \Omega_b^a} \frac{p_y}{p_0(b)} = (1-c)^k \sum_{y \in \Omega_b} \frac{p_y}{p_0(b)}.$$

Da b nun in *Aktiv* ist, erhalten wir mit 1.3

$$\mu^b(\Pi_b) \leq (1-c)^{k+1},$$

was den Induktionsschritt vervollständigt. Also gilt $\mu^a(\Pi_a) \leq (1-c)^k$ für alle $a \in Aktiv$ und $k \in \mathbb{N}$. Daraus folgt $\mu^a(\Pi_a) = 0 \ \forall a \in Aktiv$. Mit 1.2 folgt $\mu^x(\Pi_x) = 0 \ \forall x \in X$.

Es bleibt also noch zu zeigen, daß $\Gamma(x) = \{Y \mid Y \text{ ist in } x \text{ beginnender Lauf}\} \setminus Fair_\ell(x)$ als die abzählbare Vereinigung von Mengen der Form $y\Pi_x$ geschrieben werden kann. Falls $Y = x_0, x_1, \ldots \in \Gamma(x)$, so ist ℓ unendlich oft aktiv, wird aber nur endlich oft in Y angenommen. Somit gibt es also ein $i \in \mathbb{N}$ so daß gilt: falls ℓ in Schritt j angenommen wird, so ist $j < i$. Es folgt also folgende Gleichung

$$\Gamma(x) = \cup_{u \in X} \cup_{y \in \Lambda_x^u} y\Pi_u,$$

wobei Λ_x^u die Menge aller in x beginnenden und in u endenden endlichen Folgen von Zuständen in X ist. Da für $x, u \in X$ Λ_x^u abzählbar ist und $\mu^x(y\Pi_u) = 0$ für $y \in \Lambda_x^u$, erhalten wir

$$\mu^x(\Gamma(x)) \leq \sum_{u \in X} \sum_{y \in \Lambda_x^u} \mu^x(y\Pi_u) = 0.$$

Somit gilt $\mu^x(Fair_\ell(x)) = 1$ und wir erhalten $\mu^x(Fair(x)) = 1$.

□

Sei nun $Fair$ die Menge aller fairen Läufe in M. Dann ist $Fair = \cup_{x \in X} Fair(x)$ eine disjunkte Vereinigung und somit

$$\mu(Fair) = \sum_{x \in X} \mu(Fair(x)) = \sum_{x \in X} p_0(x) = 1.$$

Mit diesem mächtigen Satz können wir jetzt ganz einfach die gewünschte Aussage beweisen.

Gegeben eine endliche Markov Kette $M = (X,\ T,\ p,\ p_0)$. Sei $K_M = T$ die Menge der Markierungen und $l : X \times X \to K_M$ wie folgt definiert.

$$l(t) = t \text{ für } t \in T \text{ und } l((u,v)) = \emptyset \text{ für } (u,v) \notin T.$$

Sei $Fair^{echt}$ die Menge der echten Läufe in $Fair$. Dann gilt $\mu(Fair^{echt}) = \mu(Fair) = 1$. Wir werden jetzt zeigen, daß alle in $Fair^{echt}$ enthaltenen Läufe in einer ergodischen C Menge enden und jeden Zustand von C unendlich oft durchlaufen. Sei $Y = x_0, x_1, \ldots \in Fair^{echt}$. Dann gilt für jede Transition $(u,v) \in T$: entweder kommt u nur endlich oft in Y vor oder es gibt unendlich viele Indizes i mit $u = x_i$ und $v = x_{i+1}$. Da die Menge X endlich ist, gibt es ein $x \in X$, das unendlich oft in Y vorkommt. Nun kann man von x aus eine ergodische Menge C von M erreichen.

Sei $x, y_1, y_2, \ldots, y_n$ ein Präfix eines echten Laufes mit $y_n \in C$. Da x unendlich oft in Y vorkommt und Y fair ist, folgt, daß (x, y_1) unendlich oft in Y angenommen wird und somit y_1 unendlich oft in Y vorkommt. Induktiv erhalten wir, daß y_n unendlich oft in Y vorkommt. Es bleibt also nur noch zu zeigen, daß auch alle Zustände von C unendlich oft in Y durchlaufen werden. Da C eine starke Zusammenhangskomponente in (X, T) ist und $y_n \in C$ ist, kann man von y_n aus jeden Zustand in C erreichen. Für $c \in C$ sei n_c die kleinste natürliche Zahl, so daß man mit n_c Transitionen in C von y_n nach c gelangen kann. Sei $n = \max_{c \in C} n_c$. Da y_n unendlich oft in Y vorkommt und Y fair ist, gilt, daß alle Zustände $c \in C$ mit $n_c = 1$ unendlich oft in Y vorkommen. Induktiv erhält man, daß alle Zustände $c \in C$ mit $n_c = i$, $2 \leq i \leq n$ unendlich oft in Y vorkommen. Somit kommt jeder Zustand von C unendlich oft in Y vor, und die gewünschte Aussage ist bewiesen.

Kapitel 2

Probabilistisches *LTL*-Model Checking mit *Buechi*-Automaten

Wie wir gesehen haben, definieren LTL-Formeln über einer Menge AP von atomaren Aussagen eine Sprache von unendlichen Wörtern über dem Alphabet 2^{AP}. Um nun zu überprüfen, ob ein Transitionssystem oder ein Probabilistisches Programm eine gegebene LTL-Formel φ erfüllt, kann es hilfreich sein, die von φ erzeugte Sprache über 2^{AP} mit einem anderen Formalismus darzustellen. Eine Möglichkeit bieten hier ω-Automaten. Dies sind Automaten, die eine Sprache von unendlichen Wörtern akzeptieren.

2.1 Von einer *LTL*-Formel zum *Buechi*-Automaten

Sei Σ ein endliches Alphabet. Mit Σ^ω bezeichnen wir die Menge der unendlichen Wörter über Σ. Neben den endlichen Automaten, die Sprachen endlicher Wörter akzeptieren, gibt es nun die sogenannten ω-Automaten, die Sprachen $\subset \Sigma^\omega$ akzeptieren. Wir beschränken uns hier auf *Buechi*-Automaten, die sich von z. B. *Rabin*$-$, bzw. *Street*$-$Automaten nur in ihrer Akzeptanzbedingung unterscheiden.

Definition 2.1.1. [Nichtdeterministischer ω-Automat]
Ein nichtdeterministischer ω-Automat ist ein Tupel

$$\mathcal{A} = (Q, \Sigma, \delta, Q_0)$$

wobei

- Q eine endliche Menge von Zuständen,
- Σ ein endliches Alphabet,
- $\delta : Q \times \Sigma \to 2^Q$ eine Übergangsfunktion und
- $Q_0 \subseteq Q$ eine Menge von Anfangszuständen ist.

■

Wir nennen einen ω-Automaten *deterministisch* genau dann, wenn

$$(|\delta(q,a)| \leq 1 \; \forall q \in Q \text{ und } a \in \Sigma) \text{ und } (|Q_0| = 1).$$

Sei $V = Q$ und $E \subset V \times V$ so, daß

$$(v,w) \in E \quad \Leftrightarrow \quad \exists a \in \Sigma \; : \; w \in \delta(v,a).$$

Dann nennen wir (V,E) den *zugrundeliegenden Graphen* von $\mathcal{A}$.

Definition 2.1.2. [**Die Potenzmengenkonstruktion]**
Gegeben ein nichtdeterministischer ω-Automat $\mathcal{A} = (Q,\Sigma,\delta,Q_0)$. Wir bezeichnen mit $\mathcal{A}_{det}$ den folgenden deterministischen ω-Automaten:

$$\mathcal{A}_{det} = (2^Q,\Sigma,\delta_{det},\{Q_0\}),$$

wobei

$$\delta_{det}(P,a) = \cup_{q \in P} \delta(q,a) \quad \forall P \subset Q, \; a \in \Sigma.$$

■

$\mathcal{A}_{det}$ enthält also alle Teilmengen von Q als Zustände. Ausserdem kann man mit einem $a \in \Sigma$ von $P \subset Q$ in denjenigen Zustand gelangen, der die Vereinigung der Zustände ist, in die man in $\mathcal{A}$ mit a aus einem Zustand in P gelangen kann. Die Menge Q_0 ist der einzige Startzustand von $\mathcal{A}_{det}$.

Definition 2.1.3. [**Lauf eines ω-Automaten]**
Für ein Wort $w = a_1,a_2,\ldots$ in Σ^ω nennen wir die unendliche Zustandsfolge $s = q_0,q_1,\ldots$ einen *Lauf* von w in $\mathcal{A}$, falls $q_i \in \delta(q_{i-1},a_i)$ für $i \in \mathbb{N}$ und $q_0 \in Q_0$. Ebenso nennen wir für ein Wort $w = a_1,a_2,\ldots,a_n$ in Σ^* die endliche Zustandsfolge $s = q_0,q_1,\ldots,q_n$ einen *endlichen Lauf* von w in $\mathcal{A}$, falls $q_i \in \delta(q_{i-1},a_i)$ für $1 \leq i \leq n$ und $q_0 \in Q_0$. ■

Definition 2.1.4. [**Nichtdeterministischer *Buechi*-Automat (NBA)]**
Ein NBA ist ein Tupel

$$\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$$

wobei

- (Q, Σ, δ, Q_0) ein ω-Automat und
- $F \subseteq Q$ eine Menge von Akzeptanzzuständen ist.

■

Für einen Lauf s definieren wir die Menge der unendlich oft in s vorkommenden Zustände als $inf(s) = \{q \in Q \mid s_i = q \text{ für unendlich viele } i\}$.
Ein Lauf s in $\mathcal{A}$ heißt nun *akzeptierend*, genau dann wenn $inf(s) \cap F \neq \emptyset$, also genau dann, wenn mindestens ein Zustand der Endzustandsmenge unendlich oft in s vorkommt.

Wir sagen $\mathcal{A}$ akzeptiert die wie folgt definierte Sprache $\mathcal{L}_\omega(\mathcal{A}) \subseteq \Sigma^\omega$:

$$\mathcal{L}_\omega(\mathcal{A}) = \left\{w \in \Sigma^\omega \mid \exists \text{ akzeptierenden Lauf von } w \text{ in } \mathcal{A}\right\}.$$

Bemerke, daß man aufgrund des Nichtdeterminismus[1] mehrere Läufe für ein Eingabewort $w \in \Sigma^\omega$ haben kann. Von diesen können manche akzeptierend sein und manche nicht. Damit $w \in \mathcal{L}_\omega(\mathcal{A})$ gilt, genügt es, wenn einer dieser Läufe akzeptierend ist.

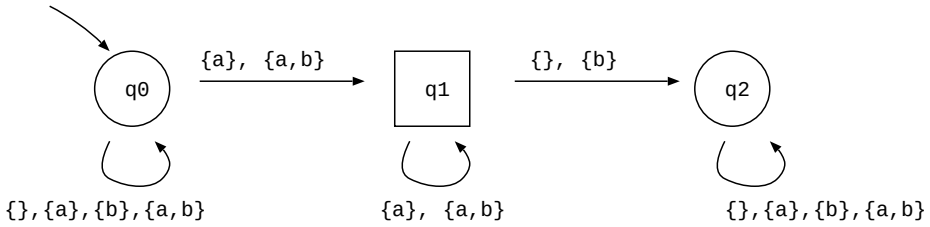
Wir nennen einen *Buechi*-Automaten *deterministisch* (DBA) genau dann, wenn der zugrundeliegende ω-Automat deterministisch ist.

Offensichtlich ist jeder DBA auch ein NBA.
Andererseits ist das Konzept der DBAs nicht so mächtig wie das der NBAs. D. h. es gibt NBAs, so daß kein DBA die gleiche Sprache akzeptiert wie der gegebene NBA. Wir können also nicht einfach durch die Potenzmengenkonstruktion einen NBA in einen DBA überführen und die gleiche Sprache erhalten.

Nun zu einem kleinen Beispiel :

[1] Für den Übergang von einem Zustand q zum nächsten mittels eines Zeichen $a \in \Sigma$ kann es mehrere Möglichkeiten geben, d. h. $|\delta(q,a)| > 1$ ist möglich.

Beispiel 2.1.1. [Beispiel für einen NBA]
Betrachte folgenden NBA $\mathcal{A}$ mit $Q = \{q_0, q_1, q_2\}$,
$\Sigma = 2^{\{a,b\}}$,
$Q_0 = \{q_0\}$,
$F = \{q_1\}$
und δ wie im folgenden Graph ersichtlich.



Wie man leicht sieht ist $\mathcal{L}_\omega(\mathcal{A})$=Words($\Diamond\Box a$) $\subset \Sigma^\omega$.[2]
Einige mögliche Läufe für $w = \{a,b\},\{a\},\{a\},\{a\},\ldots$ sind

- $q_0, q_0, q_0, q_0, \ldots$ nicht akzeptierend
- $q_0, q_1, q_1, q_1, \ldots$ akzeptierend
- $q_0, q_0, q_1, q_1, \ldots$ akzeptierend

$\vdots$

■

Wieso kann man nun *Buechi*−Automaten zum *LTL*-Model Checking benutzen?
Dies ist möglich aufgrund des folgenden, in [WVS83] gezeigten, Resultats.

Satz 2.1. *Gegeben eine LTL-Formel* φ *der Länge n über einer Menge AP. Dann gibt es einen nichtdeterministischen Buechi-Automaten* $\mathcal{A}_\varphi$ *über dem Alphabet* $\Sigma = 2^{AP}$ *mit*

$$\mathcal{L}_\omega(\mathcal{A}_\varphi) = Words(\varphi),$$

der in Zeit und Platz $O(n \cdot 2^n)$ *konstruiert werden kann.*

Da der Beweis zwar nicht schwierig, doch lang und technisch ist, verzichten wir an dieser Stelle darauf.

[2] Words($\Diamond\Box a$) ist die Menge der Wörter $w = a_1, a_2, \ldots$ über $2^\Sigma = 2^{\{a,b\}}$ so daß $\exists i \in \mathbb{N} \mid a \in a_j \; \forall j \geq i$ gilt.

2.2 *LTL*-Model Checking mit *Buechi*−Automaten

2.2.1 Nichtprobabilistisches *LTL*-Model Checking

Auch wenn diese Arbeit das Probabilistische *LTL*-Model Checking behandelt, so wollen wir doch an dieser Stelle kurz beschreiben, wie nichtprobabilistisches *LTL*-Model Checking funktioniert. Dafür benötigen wir nur noch folgende Definition.

Definition 2.2.1. [Produkttransitionssystem]
Sei $\mathcal{T} = (S, \rightarrow, S_0, AP, L)$ ein Transitionssystem und $\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$ ein NBA mit dem Alphabet 2^{AP}. Dann ist

$$\mathcal{T} \times \mathcal{A} \;=\; \left(S \times Q,\ \rightarrow_{\mathcal{T}\times\mathcal{A}}, S_0', Q, L'\right)$$

ein Transitionssystem mit folgenden Komponenten. Die Markierungsfunktion $L' : S \times Q \rightarrow 2^Q$ ist durch

$$L'(\langle s, q\rangle) \;=\; \{q\}$$

gegeben. Die Anfangszustandsmenge ist

$$S_0' \;=\; \Big\{\langle s_0, q\rangle : s_0 \in S_0, q \in \bigcup_{q_0 \in Q_0} \delta(q_0, L(s_0))\Big\}.$$

Die Transitionsrelation ist durch folgende Regel definiert:

$$\langle s, q\rangle \longrightarrow_{\mathcal{T}\times\mathcal{A}} \langle s', q'\rangle \iff (s \longrightarrow s' \;\wedge\; q' \in \delta(q, L(s')))$$

■

Intuitiv gesehen verknüpft $\mathcal{T} \times \mathcal{A}$ die Spuren von $\mathcal{T}$ mit deren Läufen in $\mathcal{A}$, d. h. , sei $\pi = (s_0, q_0), (s_1, q_1), \ldots$ ein Pfad von $\mathcal{T} \times \mathcal{A}$, dann ist $s_0, s_1, \ldots$ ein Pfad von $\mathcal{T}$ und $q_0, q_1, \ldots$ ein Lauf für dessen Spur in $\mathcal{A}$.

Sei nun $\mathcal{T} = (S, \rightarrow, S_0, AP, L)$ ein Transitionssystem und φ eine *LTL*-Formel über 2^{AP}. Mit $\mathcal{A}_\varphi$ bezeichnen wir einen NBA mit $\mathcal{L}_\omega(\mathcal{A}_\varphi) = Words(\varphi)$ (siehe Satz 2.1 auf Seite 31). Es gelten nun folgende Äquivalenzen :

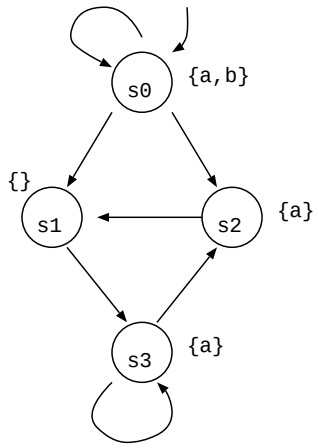
$$\mathcal{T} \models \varphi \;\Leftrightarrow\; Traces(\mathcal{T}) \subset Words(\varphi) \;\Leftrightarrow$$
$$Traces(\mathcal{T}) \cap Words(\neg\varphi) = \emptyset \;\Leftrightarrow\; Traces(\mathcal{T}) \cap \mathcal{L}_\omega(\mathcal{A}_{\neg\varphi}) = \emptyset \;\Leftrightarrow$$
$$\mathcal{T} \times \mathcal{A}_{\neg\varphi} \;\models\; \Diamond\Box\,(\wedge_{q \in F_{\mathcal{A}_{\neg\varphi}}} \neg q) \;\Leftrightarrow$$

für alle in $\mathcal{T} \times \mathcal{A}_{\neg\varphi}$ erreichbaren Zustände[3] x mit $\exists q \in F_{\mathcal{A}_{\neg\varphi}}$, so daß
x mit q markiert ist gilt : x liegt nicht auf einem Zyklus von $\mathcal{T} \times \mathcal{A}_{\neg\varphi}$

Wir sehen also, daß die Frage, ob $\mathcal{T}$ die Formel φ erfüllt auf eine Erreichsbarkeitsanalyse und Zyklentests in einem ungerichteten Graphen hinausläuft.

Zur Verdeutlichung der oben genannten Sachverhalte folgt nun ein kleines Beispiel:

Beispiel 2.2.1. Gegeben das Transitionssystem $\mathcal{T}$ mit der Menge $AP = \{a, b\}$ von atomaren Aussagen. s_0 sei der Anfangszustand von $\mathcal{T}$.



Weiterhin sei

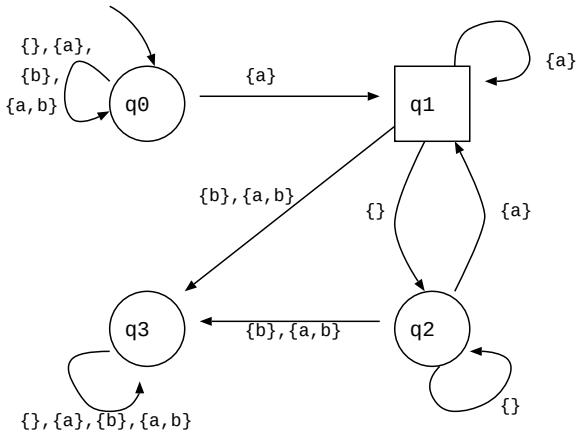
$$\varphi \;=\; \Box\Diamond a \;\longrightarrow\; \Box\Diamond b.$$

Dann gilt offensichtlich $\mathcal{T} \not\models \varphi$, da z. B. der Pfad $s_0, s_1, s_3, s_3, s_3, \ldots$ die Formel φ nicht erfüllt. Wir bilden nun die Formel $\neg\varphi$:

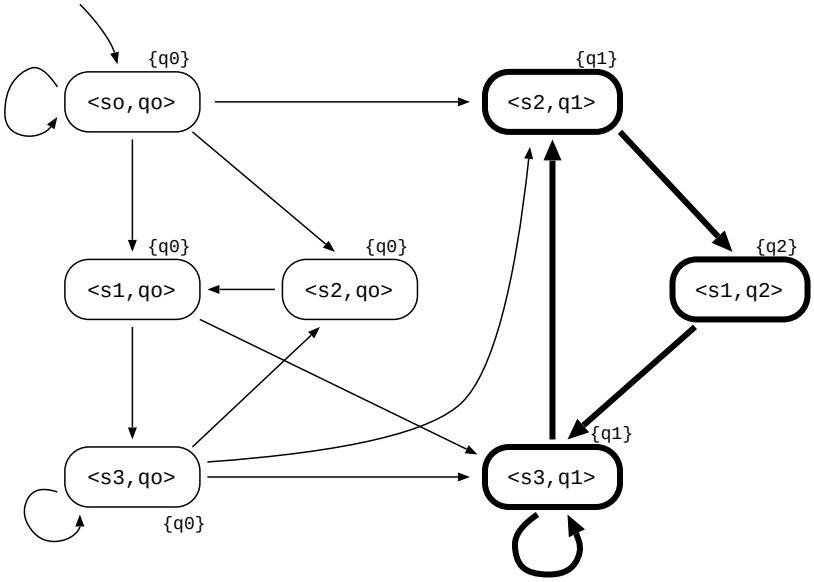
$$\neg\varphi = \neg(\neg\Box\Diamond a \;\vee\; \Box\Diamond b) =^{4}\; \Box\Diamond a \;\wedge\; \Diamond\Box\neg b.$$

Nun geben wir einen NBA $\mathcal{A}$ an, mit $\mathcal{L}_\omega(\mathcal{A}) = Words(\neg\varphi)$. Die Endzustandsmenge von $\mathcal{A}$ ist $F = \{q_1\}$.

[3] wir meinen natürlich die von einem Anfangszustand aus erreichbaren Zustände
[4] beachte, daß $=$ hier semantische Äquivalenz bedeutet



Nun erhalten wir mit obiger Konstruktionsvorschrift folgenden Produktautomaten $\mathcal{T} \times \mathcal{A}$:



Wie erwartet gibt es mit q_1 markierte erreichbare Zustände, die auf einem Zyklus liegen, d. h. $\mathcal{T} \not\models \varphi$. ■

2.2.2 Probabilistisches *LTL*-Model Checking

Gegeben ein Probabilistisches Programm $\mathcal{T}_{prob} = (M, AP, L)$ und eine LTL-Formel φ über AP. Wie schon in Definition 1.2.12 auf Seite 18 erwähnt, erfüllt $\mathcal{T}_{prob}$ die

Formel φ, wenn gilt

$$\mu(\mathbf{Y}_{\models\varphi}) = 1.$$

Wir wollen also bestimmen, ob $\mu(\mathbf{Y}_{\models\varphi}) = 1$ gilt, bzw. wir wollen den Wert von $\mu(\mathbf{Y}_{\models\varphi})$ berechnen. Wie wir bereits wissen[5], gibt es einen nichtdeterministischen *Buechi*-Automaten $\mathcal{A}_\varphi = (Q, 2^{AP}, \delta, Q_0, F)$ mit

$$\mathcal{L}_\omega(\mathcal{A}_\varphi) = Words(\varphi).$$

Definition 2.2.2. [Erfülltrelation eines Laufes von $\mathcal{T}$ bezüglich eines NBA] Sei $\mathcal{T}$ ein Probabilistisches Programm und $\mathcal{A}$ ein nichtdeterministischer *Buechi*-Automat. Sei Y ein Lauf von $\mathcal{T}$. Dann sagen wir Y erfüllt $\mathcal{A}$, i. Z. $Y \models \mathcal{A}$ genau dann, wenn

$$trace(Y) \in \mathcal{L}_\omega(\mathcal{A}).$$

Wir bezeichnen mit $\mathbf{Y}_{\models\mathcal{A}}$, bzw. $\mathbf{Y}_{\not\models\mathcal{A}}$ die Menge aller Läufe Y in $\mathcal{T}$, die $\mathcal{A}$ erfüllen, bzw. nicht erfüllen. ■

Da $\mathcal{L}_\omega(\mathcal{A}_\varphi) = Words(\varphi)$ gilt also

$$\mu(\mathbf{Y}_{\models\varphi}) = \mu(\mathbf{Y}_{\models\mathcal{A}_\varphi}).$$

Wie im nichtprobabilistischen Fall können wir auch hier mit einer Produktkonstruktion arbeiten, um den Wert $\mu(\mathbf{Y}_{\models\mathcal{A}_\varphi})$ zu ermitteln. Jedoch ist die Lage hier etwas komplizierter. Wir werden ein Pobabilistisches Programm $\mathcal{T}_{\mathcal{A}_\varphi}$ konstruieren, das sozusagen $\mathcal{T}$ simuliert, jedoch auch noch zu jedem Zeitpunkt die Information bereitstellt, in welchem Zustand sich $\mathcal{A}_\varphi$ unter Berücksichtigung der bereits besuchten Zustände befinden könnte. Aus Abschnitt 1.3.2, Seite 21 wissen wir, daß ein Lauf von $\mathcal{T}_{\mathcal{A}_\varphi}$ mit Wahrscheinlichkeit 1 in einer ergodischen Menge von $\mathcal{T}_{\mathcal{A}_\varphi}$ enden wird und jeden Zustand dieser Menge unendlich oft durchlaufen wird. Die Akzeptanzbedingung von $\mathcal{A}_\varphi$ werden wir benutzen, um die ergodischen Mengen von $\mathcal{T}_{\mathcal{A}_\varphi}$ in zwei Klassen zu einzuteilen, die Klasse der *akzeptierenden* ergodischen Mengen und die Klasse der *nicht-akzeptierenden* ergodischen Mengen. Diese Klassifizierung wird so geschehen, daß folgendes gilt:

- die Menge der Läufe, die in einer akzeptierenden ergodischen Menge enden und nicht vom NBA $\mathcal{A}_\varphi$ akzeptiert werden, bildet eine Nullmenge im Folgenraum von $\mathcal{T}_{A_\varphi}$

[5] siehe Satz 2.1, seite 31

- die Menge der Läufe, die in einer nicht-akzeptierenden ergodischen Menge enden und vom NBA $\mathcal{A}_\varphi$ akzeptiert werden, [6] bildet eine Nullmenge im Folgenraum von $\mathcal{T}_{A_\varphi}$

Es wird also gelten, daß

$$\mu(\mathbf{Y}_{\models \mathcal{A}_\varphi})$$

gleich der Wahrscheinlichkeit ist, daß ein Lauf von $\mathcal{T}_{\mathcal{A}_\varphi}$ in einer akzeptierenden ergodischen Menge von $\mathcal{T}_{\mathcal{A}_\varphi}$ endet, was einfach berechnet werden kann. Doch bis dahin bedarf es noch einiger Arbeit. Bevor wir mit der Konstruktion beginnen, wollen wir noch einige Bemerkungen/Vereinfachungen anführen.

Einige Bemerkungen/Vereinfachungen

- Als erstes werden wir die Markierungen der Zustände von $\mathcal{T}_{prob}$ und das Alphabet sowie die Übergänge des NBA $\mathcal{A}_\varphi$ ändern.

  - Sei $\mathcal{T}'_{prob} = (M, X, L')$ das Probabilistische Programm, das aus $\mathcal{T}_{prob}$ entsteht, indem man *AP* durch X ersetzt und die Markierungsfunktion folgendermassen anpaßt.

    $$L'(x) = \{x\} \quad \forall x \in X$$

  - Sei $\mathcal{A}'_\varphi = (Q, X, \delta', Q_0, F)$ ein aus $\mathcal{A}_\varphi$ entstandener NBA, wobei

    $$\delta'(q,x) = \delta(q, L(x)).$$

  Da sich die zugrundeliegende Markov Kette M nicht geändert hat, besitzen $\mathcal{T}_{prob}$ und $\mathcal{T}'_{prob}$ die gleichen Läufe und die gleiche Wahrscheinlichkeitsverteilung für diese. Zudem gilt :

  $$\mathbf{Y}_{\models \mathcal{A}_\varphi} = \mathbf{Y}'_{\models \mathcal{A}'_\varphi}. \quad (*)$$

  In Worten: die Menge der Läufe in $\mathcal{T}_{prob}$, deren Spur in $\mathcal{L}_\omega(\mathcal{A}_\varphi)$ liegt, ist gleich der Menge der Läufe in $\mathcal{T}'_{prob}$, deren Spur in $\mathcal{L}_\omega(\mathcal{A}'_\varphi)$ liegt. Somit folgt

  $$\mu(\mathbf{Y}_{\models \mathcal{A}_\varphi}) = \mu(\mathbf{Y}'_{\models \mathcal{A}'_\varphi}) = \mu'(\mathbf{Y}'_{\models \mathcal{A}'_\varphi}).$$

  Somit können wir also o. B. d. A. mit $\mathcal{T}'_{prob}$ und $\mathcal{A}'_\varphi$ weiterarbeiten.

  Zu $(*)$: Sei $Y = x_0, x_1, \ldots$ Lauf in $\mathcal{T}_{prob}$, also auch in $\mathcal{T}'_{prob}$. Es gilt:

[6] Natürlich wird nicht der Lauf selber von $\mathcal{A}_\varphi$ akzeptiert, sondern dessen Projektion auf die in $\mathcal{A}_\varphi$ liegende Komponente der Zustände. Das sehen wir dann in der Konstruktion.

$$Y \models \mathcal{A}_\varphi \;\Leftrightarrow\; \exists \text{ akzeptierenden Lauf } q_0, q_1, \ldots \text{ von } \mathit{trace}(Y) \text{ in } \mathcal{A}_\varphi \;\Leftrightarrow$$

$$\exists \text{ akzeptierenden Lauf } q_0, q_1, \ldots \text{ mit } q_i \in \delta(q_{i-1}, L(x_i)) \;\; \forall i \in \mathbb{N} \;\; \text{ in } \mathcal{A}_\varphi \;\Leftrightarrow$$

$$\exists \text{ akzeptierenden Lauf } q_0, q_1, \ldots \text{ mit } q_i \in \delta'(q_{i-1}, x_i) \;\; \forall i \in \mathbb{N} \;\; \text{ in } \mathcal{A}'_\varphi \;\Leftrightarrow$$

$$\exists \text{ akzeptierenden Lauf } q_0, q_1, \ldots \text{ von } \mathit{trace}(Y) \text{ in } \mathcal{A}'_\varphi \;\Leftrightarrow\; Y \models \mathcal{A}'_\varphi,$$

womit die Behauptung folgt.

- Ausserdem werden wir im folgenden annehmen, daß $\mathcal{A}'_\varphi$ in jedem Zustand für jeden Buchstaben $x \in X$ mindestens einen Übergang besitzt. Dies kann man o. B. d. A. tun, da man Übergänge zu einem zusätzlichen Zustand einfügen kann, der nicht in der Akzeptanzmenge liegt.

- Damit die späteren Konstruktionen übersichtlicher bleiben, wollen wir, daß $\mathcal{A}'_\varphi$ nur einen Anfangszustand besitzt. Dies können wir wie folgt erreichen: Sei $\mathcal{A}''_\varphi = (Q \cup \{q_0\}, X, \delta'', \{q_0\}, F)$ ein aus $\mathcal{A}'_\varphi$ entstandener NBA, wobei $q_0 \notin Q$,
$$\delta''(q,x) = \delta'(q,x) \quad \forall q \in Q \wedge x \in X \;\text{ und}$$
$$\delta''(q_0,x) = \cup_{q \in Q_0} \delta'(q,x), \quad \forall x \in X.$$
Es wird also nur ein neuer (und einziger) Startzustand eingefügt, der genau die Übergänge der alten Startzustände besitzt. Daß sich dadurch die vom Automaten akzeptierte Sprache nicht ändert, ist offensichtlich.

- Dieser Punkt betrifft nur die Notation. Aus Gründen der Übersichtlichkeit werden wir im folgenden für die Menge $\{(x,q) \mid q \in R\}$ die abkürzende Schreibweise (x,R) verwenden.

Damit die Notation nicht zu kompliziert wird, fangen wir mit dieser sozusagen noch einmal von vorne an.
Sei $\mathcal{T}_{prob} = (M, X, L)$ ein Probabilistisches Programm mit $M = (X, T, p, p_0)$ und $\mathcal{A} = (Q, X, \delta, \{q_0\}, F)$ ein nichtdeterministischer *Buechi*-Automat, so daß $\mathcal{T}_{prob}$ und $\mathcal{A}$ die drei oben genannten Punkte erfüllen. Da $\mathcal{L}_\omega(\mathcal{A})$ gleich der von einer

LTL-Formel erzeugten Sprache sein soll, gelte $\mathcal{L}_\omega(\mathcal{A})$ ist messbar im Folgenraum von M.[7] Also ist die Aufgabe, den Wert

$$\mu(\mathbf{Y}_{\models\mathcal{A}})$$

zu berechnen.

Die Konstruktion

Als erstes bilden wir das Produkttransitionssystem $\mathcal{T}_{prob} \times \mathcal{A}$ wie in Definition 2.2.1, Seite 32 beschrieben.[8] Nun können wir $\mathcal{T}_{prob} \times \mathcal{A}$ auch als nichtdeterministischen ω-Automaten über dem Alphabet X mit folgender Übergangsfunktion ρ betrachten:

$$\rho((x,q),\tilde{x}) \;=\; \{(\tilde{x},\tilde{q}) \mid \tilde{q} \in \delta(q,\tilde{x})\}, \;\text{ falls } (x,\tilde{x}) \in T.$$

Bemerke, daß in einen Zustand (x,q) nur Transitionen mit dem Buchstaben x hineinführen. Somit gilt für einen Zustand $P \subset X \times Q$ des durch Potenzmengenkonstruktion (siehe Definition 2.1.2, Seite 29) erhalten Automaten $(\mathcal{T}_{prob} \times \mathcal{A})_{det}$: führt eine Transition mit dem Buchstaben x nach P, so enthält P nur Paare, deren erste Komponente x ist. Da abgesehen vom Startzustand also nur Knoten der Art $\{(x,r) \mid r \in R\} = (x,R)$, mit $R \subset Q$, erreichbar sind, werden wir bei der Potenzmengenkonstruktion abgesehen vom Startzustand auch nur solche Knoten berücksichtigen. Nun wollen wir aber aus technischen Gründen, daß auch der Startzustand von der Art (x,R), $R \subset Q$ ist. Dies ist nicht gegeben, denn i. Allg. enthält der Startzustand Zustände von $(\mathcal{T}_{prob} \times \mathcal{A})$ mit unterschiedlicher erster Komponente. Wir können unser Ziel dennoch erreichen, indem wir für jede dieser Komponenten einen eigenen Startzustand definieren und gegebenfalls einfügen. Wir erhalten dann einen *semideterministischen* Automaten, d. h. einen Automaten mit deterministischer Übergangsfunktion, aber mit mehreren Anfangszuständen. Dies stellt aber in unseren weiteren Überlegungen kein Problem dar. Wir nehmen also folgende Modifikation vor:

Definition 2.2.3. [Der Automat $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$]
Sei y der Startzustand von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}$. Sei $Komp \subset X$ so, daß $x \in Komp$ als

[7] Es ist zwar allgemein bekannt, daß die von einem NBA akzeptierte Sprache messbar ist im Folgenraum einer Markov Kette (siehe [Va85]), jedoch genügt hier schon die schwächere Aussage über die Messbarkeit der Sprache einer LTL-Formel.

[8] Wobei $\mathcal{T}_{prob}$ auf offensichtliche Weise mit $\{x \in X \mid p_0(x) > 0\}$ als Menge der Anfangszustände als Transitionssystem betrachtet wird.

erste Komponente eines Elementes von y vorkommt, also

$$Komp \;=\; \{x \in X \mid \exists q \in Q \;:\; (x,q) \in y\}.$$

Wir definieren

$$(\mathcal{T}_{prob} \times \mathcal{A})_{sdet} \;=\; (Q'', X, \rho'', Q_0''),$$

mit

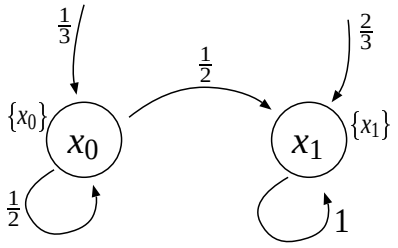
- $Q'' \;=\; \{(x,R) \mid x \in X, R \subset Q\} \;=\; X \times 2^Q$
- $Q_0'' \;=\; \{(x,Q) \cap y \;\mid\; x \in Komp\}$
- $\rho''((x,R),x') \;=\; \cup_{r \in R}\, \rho((x,r),x')$

Wir haben also eigentlich nur den Startzustand von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}$ in mehrere Teile bezüglich ihrer ersten Komponente aufgeteilt und die trivialerweise nicht erreichbaren Knoten (solche, die Knoten von $\mathcal{T}_{prob} \times \mathcal{A}$ mit verschiedenen ersten Komponenten enthalten) weggelassen. ■

Wir bezeichnen für $\{(x,q)\} \in Q''$ mit $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ denjenigen Teil von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$, der vom Zustand $\{(x,q)\}$ aus erreichbar ist. Zusätzlich sei $\{(x,q)\}$ der Anfangszustand von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$.

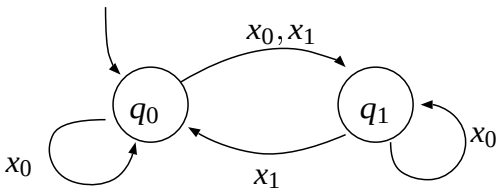
Zur Erinnnerung daran, wie die Konstruktionen durchzuführen sind, folgt jetzt ein Beispiel. Gegeben seien ein Probabilistisches Programm

$\mathcal{T}_{prob}$:



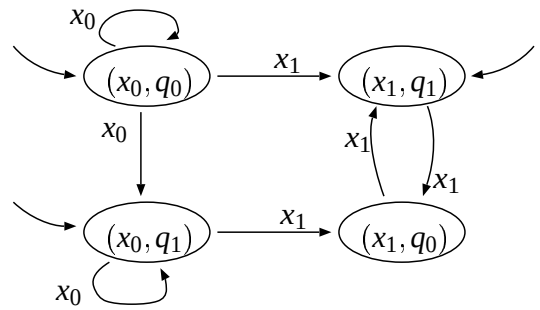
und ein NBA

$\mathcal{A}$:



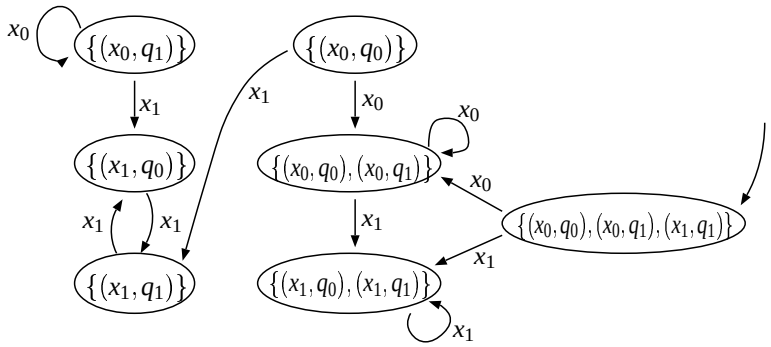
mit den gewünschten Eigenschaften. Dann erhalten wir folgendes Produktsystem,

$\mathcal{T}_{prob} \times \mathcal{A}$:



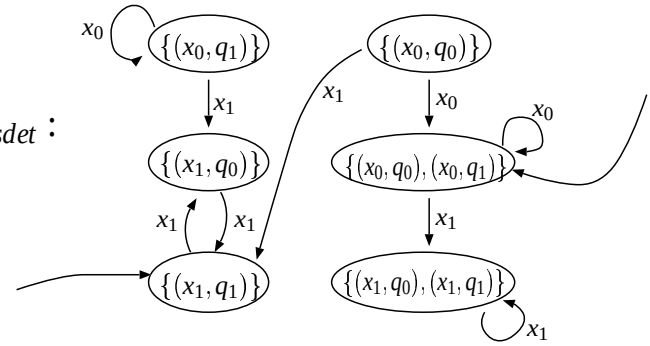
auf welches wir die Potenzmengenkonstruktion anwenden können. Dies ergibt dann:

$(\mathcal{T}_{prob} \times \mathcal{A})_{det}$:



Zum Schluss dann noch das Aufsplitten des Startzustandes.

$(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$:



Wir werden uns jetzt überlegen, welcher Zusammenhang zwischen den Läufen von $\mathcal{T}_{prob} \times \mathcal{A}$, bzw. $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$ und den Läufen von M besteht.

- Sei $Y' = (x_0, q_0), (x_1, q_1), \ldots$ ein Lauf in $\mathcal{T}_{prob} \times \mathcal{A}$. Dann nennen wir $x_0, x_1, \ldots$ den (eindeutigen) zu Y' *korrespondierenden* (echten) Lauf in $\mathcal{T}$.

- Sei $Y'' = (x_0,Q_0),(x_1,Q_1),\ldots$ ein Lauf in $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$. Dann nennen wir $x_0,x_1,\ldots$ den (eindeutigen) zu Y'' *korrespondierenden* (echten) Lauf in $\mathcal{T}$.

Sei nun $Y = x_0,x_1,x_2,\ldots$ ein Lauf in $\mathcal{T}_{prob}$.

- Sei (x_0,q_0) ein Zustand von $\mathcal{T}_{prob} \times \mathcal{A}$. Dann gibt es in $\mathcal{T}_{prob} \times \mathcal{A}$ mindestens einen in (x_0,q_0) beginnenden Lauf Y', so daß Y korrespondierender Lauf zu Y' ist (siehe Definition von $\mathcal{T}_{prob} \times \mathcal{A}$ und bemerke, daß $\mathcal{A}$ in jedem Zustand für jeden Buchstaben $x \in X$ mindestens einen Übergang besitzt).

- Sei (x_0,Q_0) ein Zustand von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$. Dann gibt es in $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$ genau einen in (x_0,Q_0) beginnenden Lauf Y'', so daß Y korrespondierender Lauf zu Y'' ist (siehe Definition von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$ und bemerke, daß $\mathcal{A}$ in jedem Zustand für jeden Buchstaben $x \in X$ mindestens einen Übergang besitzt).

Bemerkung 5. Sei $Y'' = \{(x_0,q_0)\},(x_1,Q_1),\ldots$ ein Lauf in $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$ (bemerke, daß der Startzustand einelementig ist). Seien $i \in \mathbb{N}$ und $(x_i,q_i) \in (x_i,Q_i)$ beliebig. Dann gibt es $(x_j,q_j) \in (x_j,Q_j)$ für $j = 1,2,\ldots,i-1$, so daß es im zugrundeliegenden Graphen von $\mathcal{T}_{prob} \times \mathcal{A}$ den Weg $(x_0,q_0)(x_1,q_1)\ldots(x_i,q_i)$ gibt, genauer gilt $(x_k,q_k) \in \rho((x_{k-1},q_{k-1}),x_k)$, $k = 1,2,\ldots,i$. Dies ist offensichtlich, da der Startzustand von Y'' einelementig ist und somit induktiv alle Elemente von (x_k,Q_k) im zugrundeliegenden Graphen von $\mathcal{T}_{prob} \times \mathcal{A}$ durch einen solchen Weg von (x_0,q_0) erreicht werden können.

Wie wir bereits erwähnt haben, betrachten wir $\mathcal{T}_{prob} \times \mathcal{A}$ als nichtdeterministischen ω-Automaten mit Übergangsfunktion ρ. Nun werden wir noch geeignet die Akzeptanzbedingung von $\mathcal{A}$ hinzufügen, so daß $\mathcal{T}_{prob} \times \mathcal{A}$ zum *Buechi*-Automaten wird. Als Menge der Akzeptanzzustände wählen wir $X \times F$, wobei F die Menge der Akzeptanzzustände von $\mathcal{A}$ ist. Wir erhalten also einen *NBA* bestehend aus dem Tupel $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA} = ((X \times Q),\ X,\ \rho,\ X_0',\ X \times F))$, wobei X_0' wie in Definition 2.2.1, Seite 32 definiert ist. Es gilt nun :

Lemma 2.1. *Sei $Y = x_0,x_1,x_2,\ldots$ ein echter Lauf von $\mathcal{T}$. Dann gilt: $x_0,x_1,x_2,\ldots \in \mathcal{L}_\omega(\mathcal{A}) \Leftrightarrow \exists$ akzeptierenden Lauf Y' in $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$, so daß Y korrespondierender Lauf zu Y' ist.*

Beweis :

"$\Longrightarrow$": $Y \in \mathcal{L}_\omega(\mathcal{A})$, es gibt also einen akzeptierenden Lauf $q_{-1},q_0,q_1,\ldots$ von $\mathcal{A}$ mit $q_i \in \delta(q_{i-1},x_i)$ $\forall i = 0,1,2,\ldots$ Da Y akzeptierend ist in $\mathcal{A}$, gibt es einen

Akzeptanzzustand $q_F \in F$ der unendlich oft in Y vorkommt, es gibt also Indizes $i_1 < i_2 < i_3 < \ldots$ mit $q_{i_k} = q_F \quad \forall k \in \mathbb{N}$. Nun ist $Y' = (x_0,q_0),(x_1,q_1),\ldots$ ein Lauf in $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ zu dem Y korrespondiert. Wir müssen also nur noch zeigen, daß Y' von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ akzeptiert wird. Es gilt für alle $k \in \mathbb{N}$, daß $(x_{i_k}, q_{i_k}) = (x_{i_k}, q_F) \in X \times F$. Da $X \times F$ eine endliche Menge ist (beide Komponenten sind endlich), folgt nun, daß mindestens ein Element von $X \times F$ in $((x_{i_k}, q_F),\ k \in \mathbb{N})$ unendlich oft vorkommt, und Y' wird von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ akzeptiert.
"$\Longleftarrow$": sei $Y' = (x_0,q_0),(x_1,q_1),\ldots$ akzeptierender Lauf in $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$. Es gibt also einen Zustand (x_F,q_F) aus $X \times F$ der unendlich oft in Y' vorkommt. Sei Y der zu Y' korrespondierende Lauf in $\mathcal{A}$, also $Y = x_0,x_1,\ldots$. Da (x_0,q_0) ein Anfangszustand von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ ist, gibt es einen Anfangszustand q_{-1} von $\mathcal{A}$ mit $q_0 \in \delta(q_{-1},x_0)$. Weiterhin gilt $q_i \in \delta(q_{i-1},x_i) \quad \forall i \in \mathbb{N}$.[9] Es ist also $q_{-1},q_0,q_1,\ldots$ ein Lauf für Y in $\mathcal{A}$. Es bleibt also noch zu zeigen, daß $q_{-1},q_0,q_1,\ldots$ akzeptierend ist in $\mathcal{A}$. Da jedoch $(x_F,q_F) \in X \times F$ unendlich oft in Y' vorkommt, kommt offensichtlich $q_F \in F$ unendlich oft in Y vor. Somit ist die Behauptung gezeigt. □

Wir zerlegen nun $\mathbf{Y}_{\models\mathcal{A}}$ folgendermassen: sei $\mathbf{Y}'_{\models\mathcal{A}}$ die Menge

$$\mathbf{Y}'_{\models\mathcal{A}} = \{Y = x_0,x_1,\ldots \in \mathbf{Y}_{\models\mathcal{A}} \mid Y \text{ echter Lauf in } \mathcal{T}\}. \quad [10]$$

Also gilt

$$\mathbf{Y}_{\models\mathcal{A}} = \mathbf{Y}'_{\models\mathcal{A}} \cup \mathit{Rest},$$

wobei *Rest* eine Teilmenge der nicht echten Läufe von $\mathcal{T}_{prob}$ und somit eine Nullmenge im Folgenraum von $\mathcal{T}$ ist. Wir erhalten also

$$\mu(\mathbf{Y}_{\models\mathcal{A}}) \;=\; \mu(\mathbf{Y}'_{\models\mathcal{A}}). \tag{2.1}$$

Da es aufgrund des eben oben gezeigten Lemma eine "genau dann, wenn " Beziehung zwischen den Läufen in $\mathbf{Y}'_{\models\mathcal{A}}$ und den akzeptierenden Läufen von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ gibt, liegt es nahe, den Wert $\mu(\mathbf{Y}'_{\models\mathcal{A}})$ mittels den akzeptierenden Läufen von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ zu bestimmen. Dafür gehen wir jetzt folgendermassen vor. Wir definieren für jeden Akzeptanzzustand $(x_F,q_F) \in X \times F$ die Menge

$$\mathcal{L}((x_F,q_F)) \;\subset\; \mathcal{L}_\omega((\mathcal{T}_{prob} \times \mathcal{A})_{NBA})$$

[9] Bemerke, daß Y echter Lauf in $\mathcal{T}$ ist .
[10] bemerke $trace(Y) = Y$

der Wörter aus X^ω, für die es einen Lauf in $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ gibt, der unendlich oft (x_F, q_F) durchläuft,
$\mathcal{L}((x_F, q_F)) = \{Y \in X^\omega \mid \exists$ Lauf $a_0, a_1, \ldots$ für Y in $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$
mit $a_i = (x_F, q_F)$ für unendlich viele $i\}$.
Nun kann natürlich sein, daß für ein $(x_F, q_F) \in X \times F$ die Menge $\mathcal{L}((x_F, q_F))$ in $\mathcal{T}_{prob}$ die Wahrscheinlichkeit 0 besitzt, daß also

$$\mu(\mathcal{L}((x_F, q_F))) = 0.$$

Solche Teilmengen von $\mathcal{L}_\omega((\mathcal{T}_{prob} \times \mathcal{A})_{NBA})$ tragen offensichtlich nichts zum Wert von $\mu(\mathcal{L}_\omega((\mathcal{T}_{prob} \times \mathcal{A})_{NBA}))$ bei. Wir werden nun die Akzeptanzzustände (x_F, q_F) von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ charakterisieren, für die die Sprache $\mathcal{L}((x_F, q_F))$ positives μ-Maß hat.

Definition 2.2.4. [**Periodische Zustände]**
Ein Zustand (x, q) von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ heißt *periodisch,* falls der zugrundeliegende Graph von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x, q))$ eine ergodische Menge C mit folgender Eigenschaft enthält: $\exists\, R \in C \mid (x, q) \in R$.
Für einen periodischen Zustand (x, q) sei $\gamma_{(x,q)} \in X^*$ ein endliches Wort über X, so daß $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x, q))$ durch Eingabe von $\gamma_{(x,q)}$ von $\{(x, q)\}$ zu einem Zustand in C übergeht. ■

Bemerke, daß es i. Allg. eine unendliche Anzahl an Wörtern aus X^* gibt, die die Anforderungen an $\gamma_{(x,q)}$ erfüllen. $\gamma_{(x,q)}$ sei ein beliebiges solches festes Wort. Bemerke ausserdem, daß für $\gamma_{(x,q)} = x_0, x_1, \ldots, x_n$ die (x_{i-1}, x_i) Transitionen in $\mathcal{T}_{prob}$ sind, also $(x_{i-1}, x_i) \in T$, $i = 1, 2, \ldots, n$.

Bevor wir nun fortfahren, wollen wir noch erklären, wie man für gegebenes $(x, q) \in X \times Q$ den zugrundeliegenden Graphen von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x, q))$ als Markov Kette interpretieren kann. Dazu folgende Definition:

Definition 2.2.5. [**Die Markov Kette $M'_{(x,q)}$]**
Sei $(x, q) \in X \times Q$. Sei $G = (V, E)$ der zugrundeliegende Graph von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x, q))$. Dann definieren wir $M'_{(x,q)}$ als

$$M'_{(x,q)} = (V, E, \tilde{p}, \tilde{p}_0),$$

wobei

- $\tilde{p}((x, R), (x', R')) = p_{xx'}$ für $((x, R), (x', R')) \in E$.

- $\tilde{p}_0(\{(x,q)\}) = 1.$

Dann ist $M'_{(x,q)}$ eine endliche Markov Kette.

Wir bezeichnen mit $\mu'_{(x,q)}$ das Wahrscheinlichkeitsmaß des Folgenraums von $M'_{(x,q)}$. ■

Definition 2.2.6. [Das Ereignis $\mathbf{Wdh}_1$]
Seien $x_{wdh} \in X$ und $q_{wdh} \in Q$. $\mathbf{Wdh}_1$ sei das Ereignis, daß ein in x_{wdh} beginnender Lauf Y von $\mathcal{T}_{prob}$ zu einem Lauf Y' von $\mathcal{T}_{prob} \times \mathcal{A}$ korrespondiert, der in (x_{wdh}, q_{wdh}) beginnt und (x_{wdh}, q_{wdh}) unendlich oft durchläuft. ■

Lemma 2.2. *Sei (x,q) periodisch und $\gamma_{(x,q)} = \tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n$ das mit (x,q) assoziierte Wort aus X^*. Das System $\mathcal{T}_{prob}$ starte in x. Dann ist die Wahrscheinlichkeit für das Ereignis $\mathbf{Wdh}_1$ mit $x_{wdh} = x$ und $q_{wdh} = q$ unter der Bedingung, daß $\mathcal{T}_{prob}$ zuerst die Transitionen in $\gamma_{(x,q)}$ durchläuft, gleich 1.*
Beweis : Sei $p(\gamma_{(x,q)})$ die Wahrscheinlichkeit, daß ein in x beginnender Lauf von $\mathcal{T}_{prob}$ das Wort $\gamma_{(x,q)}$ als Präfix hat, also

$$p(\gamma_{(x,q)}) = \frac{p_{\gamma_{(x,q)}}}{p_0(x)} = p_{x\tilde{x}_1} \cdot p_{\tilde{x}_1\tilde{x}_2} \cdot \ldots \cdot p_{\tilde{x}_{n-1}\tilde{x}_n}.$$ [11]

Da, wie oben schon erwähnt, die $(\tilde{x}_{i-1}, \tilde{x}_i) \in T$ für $i = 1,2,\ldots,n$ (mit $\tilde{x}_0 = x$), gilt

$$p(\gamma_{(x,q)}) > 0.$$

Wir werden jetzt zeigen, daß man mit Wahrscheinlichkeit 1 für jeden Lauf Y von $\mathcal{T}_{prob}$, der das Wort $x\gamma_{(x,q)}$ als Präfix hat, einen Lauf Y' von $\mathcal{T}_{prob} \times \mathcal{A}$ konstruieren kann, so daß Y der zu Y' korrespondierende Lauf ist und Y' in (x,q) beginnt und (x,q) unendlich oft durchläuft. Dazu zeigen wir, daß man mit Wahrscheinlichkeit 1 den Lauf Y folgendermassen unterteilen kann: $Y = xt_1xt_2xt_3\ldots$, wobei jedes t_i, $i \in \mathbb{N}$ das Wort $\gamma_{(x,q)}$ als Präfix besitzt. Zusätzlich wird es einen zu Y korrespondierenden Lauf $Y' = y_0, y_1, y_2, \ldots$ von $\mathcal{T}_{prob} \times \mathcal{A}$ geben, der in (x,q) beginnt und sich am Ende jedes Segments im Zustand (x,q) befindet, d. h. $y_k = (x,q) \quad \forall k = \sum_{j=1}^{i}(|t_j|+1)$, $i = 0,1,2,\ldots$. Damit ist dann die Aussage des Lemmas gezeigt.

Sei also nun $Y = X_0, X_1, X_2, \ldots$ ein Lauf von M (also auch von $\mathcal{T}_{prob}$), der das Wort $x\gamma_{(x,q)}$ als Präfix hat. Die erwähnte Unterteilung wird schrittweise geschehen und wir werden Teilresultate mittels vollständiger Induktion zeigen. Sei $\mathbf{divide}_i$ das Ereignis, daß man Y in $xt_1xt_2x\ldots xt_ixRest_i$ unterteilen kann, mit $Rest_i$ hat das

[11] siehe Bemerkung 4, seite 18

Wort $\gamma_{(x,q)}$ als Präfix, und t_k hat das Wort $\gamma_{(x,q)}$ als Präfix, $k = 1,2,\ldots,i$, und es gibt endlichen in (x,q) beginnenden Lauf $y_0,y_1,\ldots,y_m,\ m = \sum_{j=1}^{i}(|t_j|+1)$ von $\mathcal{T}_{prob} \times \mathcal{A}$, der mit dem Präfix $X_0,X_1,\ldots,X_m$ von Y korrespondiert und für den gilt: $y_k = (x,q) \quad \forall k = \sum_{j=1}^{l}(|t_j|+1),\ l = 0,1,2,\ldots,i$.
Behauptung 1 : Die Wahrscheinlichkeit für das Ereignis **divide**$_i$ für beliebiges $i \in \mathbb{N}$ ist gleich 1.
Bew.: mittels vollständiger Induktion über i

- Induktionsanfang : i = 0.
  Hier gibt es nichts zu zeigen, da Y das Wort $x\gamma_{(x,q)}$ als Präfix hat. Also genügt die Unterteilung $Y = xRest_0$ (bemerke, daß $X_0 = x$ und $Rest_0$ beginnt mit $\gamma_{(x,q)}$). Ausserdem ist $y_0 = (x,q)$ der gewünschte endliche Lauf von $\mathcal{T}_{prob} \times \mathcal{A}$.

- Induktionsschritt : es gelte **divide**$_i$ mit Wahrscheinlichkeit 1
  D. h. mit Wahrscheinlichkeit 1 haben wir $Y = xt_1xt_2x\ldots xt_ixRest_i$ mit $Rest_i$ hat das Wort $\gamma_{(x,q)}$ als Präfix, und t_k hat das Wort $\gamma_{(x,q)}$ als Präfix, $k = 1,2,\ldots,i$, und es gibt endlichen in (x,q) beginnenden Lauf $y_0,y_1,\ldots,y_m,\ m = \sum_{j=1}^{i}(|t_j|+1)$ von $\mathcal{T}_{prob} \times \mathcal{A}$, der mit dem Präfix $X_0,X_1,\ldots,X_m$ von Y korrespondiert und für den gilt: $y_k = (x,q) \quad \forall k = \sum_{j=1}^{l}(|t_j|+1),\ l = 0,1,2,\ldots,i$.
  Wir betrachten jetzt den Lauf $\widehat{Y} = X_m,X_{m+1},\ldots = xRest_i$ von M. Dann hat $\widehat{Y}$ das Wort $x\gamma_{(x,q)}$ als Präfix. Es sei $Y'' = Y_m,Y_{m+1},\ldots$ der korrespondierende in $\{(x,q)\}$ beginnende Lauf in $M'_{(x,q)}$ (bemerke, daß Y'' eindeutig ist). Sei $d > m \in \mathbb{N}$ nun minimal, so daß gilt:

  - $(x,q) \in Y_d$
  - $X_{d+1}\ldots X_{d+n} = \gamma_{(x,q)}$

  Behauptung 2 : d ist mit Wahrscheinlichkeit 1 endlich.
  Bew.: Da (x,q) periodisch ist gibt es eine ergodische Menge C von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ die einen Zustand y enthält, mit $(x,q) \in y$. Nun sind die zugrundeliegenden Graphen von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ und $M'_{(x,q)}$ aber die gleichen. Also ist C auch ergodische Menge von $M'_{(x,q)}$. Ausserdem ist $\gamma_{(x,q)}$ gerade so gewählt, daß ein Lauf für das Eingabewort $\gamma_{(x,q)}$ in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ in C endet. Da $\widehat{Y}$ das Wort $x\gamma_{(x,q)}$ als Präfix hat und korrespondierender Lauf zu Y'' ist, folgt somit auch, daß $Y_m \in C$ gilt. Wir wissen, daß Y'' mit Wahrscheinlichkeit 1 jeden Zustand von C unendlich oft durchlaufen wird (siehe Abschnitt 1.3.2, Seite 21). Also wird auch der Zustand y

mit Wahrscheinlichkeit 1 unendlich oft von Y'' durchlaufen. Sei also $Y_k = y$ für ein $k \in \mathbb{N}$. Da $y = (x,R)$ für ein $R \subset Q$, folgt $X_k = x$. Somit erhalten wir (bemerke, daß $\gamma_{(x,q)} = \tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n$ vorausgesetzt war):

$$\mu'_{(x,q)}(Y_{k+1} = (\tilde{x}_1, R_1), \ldots, Y_{k+n} = (\tilde{x}_n, R_n) | Y_k = (x,R) = y)$$

$$= {}^{12}\mu(X_{k+1} = \tilde{x}_1, \ldots, X_{k+n} = \tilde{x}_n | X_k = x) \; = {}^{13}\; \mu(X_1 = \tilde{x}_1, \ldots, X_n = \tilde{x}_n | X_0 = x)$$

$$= p(\gamma_{(x,q)}) > 0$$

Falls also Y'' in Schritt k den Zustand y erreicht hat, so ist die Wahrscheinlichkeit, daß Y'' in den Schritten $k+1, \ldots, n$ die Zustände $(\tilde{x}_1, R_1), \ldots, (\tilde{x}_n, R_n)$ erreicht, echt größer als 0. Da Y'' aber mit Wahrscheinlichkeit 1 den Zustand y unendlich oft durchläuft, ist die Wahrscheinlichkeit, daß die Sequenz $Y_k = y, Y_{k+1} = (\tilde{x}_1, R_1), \ldots, Y_{k+n} = (\tilde{x}_n, R_n)$ für beliebiges $k \in \mathbb{N}$ nicht in Y'' vorkommt, gleich 0. Somit gibt es mit Wahrscheinlichkeit 1 ein $d \in \mathbb{N}$ mit $Y_d = y, Y_{d+1} = (\tilde{x}_1, R_1), \ldots, Y_{d+n} = (\tilde{x}_n, R_n)$, also auch

- $(x,q) \in Y_d$
- $X_{d+1} \ldots X_{d+n} \; = \; \gamma_{(x,q)}$

Damit ist die Behauptung 2 gezeigt.

Wir können nun den nächsten Schritt der Unterteilung von Y vornehmen. Sei $t_{i+1} = X_{m+1}, \ldots, X_{d-1}$. Dann hat t_{i+1} wie gewünscht das Wort $\gamma_{(x,q)}$ als Präfix. Zudem hat der Rest von Y, also $X_d, X_{d+1}, \ldots$, wieder das Wort $x\gamma_{(x,q)}$ als Präfix. Somit gilt für dir Unterteilung $Y = xt_1xt_2x \ldots xt_ixt_{i+1}xRest_{i+1}$, daß $Rest_{i+1}$ das Wort $\gamma_{(x,q)}$ als Präfix hat. Wir können nun auch den endlichen Lauf $y_0, y_1, \ldots, y_m$ wie gefordert verlängern. Nach Konstruktion gilt $Y_m, Y_{m+1}, \ldots, Y_d$ ist Präfix eines Laufes von $M'_{(x,q)}$, so auch von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$, mit $Y_m = \{(x,q)\}$ und $(x,q) \in Y_d$. Somit gilt mit Bemerkung 5, Seite 41, daß es in $\mathcal{T}_{prob} \times \mathcal{A}$ einen in (x,q) beginnenden Lauf $\widetilde{Y}' = a_m, a_{m+1}, \ldots, a_d, a_{d+1}, a_{d+2}, \ldots$ gibt, so daß $a_d = (x,q)$ und die erste Komponente von a_i gleich der ersten Komponente von Y_i ist, für $i = m, m+1, \ldots, d$. Da nun $\widehat{Y}$ zu Y'' korrespondiert gilt dies auch für die Sequenzen $X_m, X_{m+1}, \ldots, X_d$ und $a_m, a_{m+1}, \ldots, a_d$. Somit sei also $a_{m+1}, \ldots, a_d$ der nächste Teil von Y', also

$$y_{m+1} = a_{m+1}, \quad y_{m+2} = a_{m+2}, \quad \ldots\ldots, \quad y_d = a_d.$$

[12] beachte die Konstruktion von $M'_{(x,q)}$ und die Eindeutigkeit von Y'' (bzgl. Y)

[13] wegen der Markov Eigenschaft

Setzen wir Ereignis $\mathbf{divide}_i$ voraus, so gilt Ereignis $\mathbf{divide}_{i+1}$ also mit Wahrscheinlichkeit 1. Da nun aber schon das Ereignis $\mathbf{divide}_i$ mit Wahrscheinlichkeit 1 gilt, können wir induktiv folgern, daß auch das Ereignis $\mathbf{divide}_{i+1}$ mit Wahrscheinlichkeit 1 gilt. Somit ist Behauptung 1 also gezeigt.

Nun gilt aber auch[14], daß die Wahrscheinlichkeit für das Ereignis $\bigcap_{i=0,1,\ldots} \mathbf{divide}_i$ gleich 1 ist. Das bedeutet aber nichts anderes, als daß wir mit Wahrscheinlichkeit 1 einen Lauf Y mit Präfix $x\gamma_{(x,q)}$ in unendlich viele Segmente der geforderten Art unterteilen können und einen zu Y korrespondierenden Lauf Y' von $\mathcal{T}_{prob} \times \mathcal{A}$ angeben können, so daß Y' den Zustand (x,q) unendlich oft durchläuft. Damit ist die Aussage des Lemmas gezeigt.

□

Bevor wir nun zu einem zusammenfassenden Resultat kommen können, benötigen wir noch ein weiteres Lemma, das Aussagen über das Akzeptanzverhalten nicht periodischer Zustände macht. Dazu definieren wir uns zuerst ein neues Wiederholungsereignis und zeigen dann ein solches Lemma.

Definition 2.2.7. [Das Ereignis $\mathbf{Wdh}_2$]
Seien $x_{wdh}, x_{start} \in X$ und $q_{wdh}, q_{start} \in Q$. $\mathbf{Wdh}_2$ sei das Ereignis, daß ein in x_{start} beginnender Lauf Y von $\mathcal{T}_{prob}$ zu einem Lauf Y' von $\mathcal{T}_{prob} \times \mathcal{A}$ korrespondiert, der in (x_{start}, q_{start}) beginnt und (x_{wdh}, q_{wdh}) unendlich oft durchläuft. ■

Lemma 2.3. *Sei (x,q) nicht periodisch. Dann gilt für beliebiges $(x_{start}, q_{start}) \in X \times Q$, daß das Ereignis $\mathbf{Wdh}_2$ mit $x_{wdh} = x$ und $q_{wdh} = q$ mit Wahrscheinlichkeit 0 eintritt.*
Beweis :

- $(x_{start}, q_{start}) = (x_{wdh}, q_{wdh}) = (x,q)$
  Sei $Y = X_0, X_1, X_2, \ldots$ ein Lauf in M (also auch $\mathcal{T}_{prob}$) mit $X_0 = x$. Es sei $Y'' = Y_0, Y_1, Y_2, \ldots$ der eindeutige zu Y korrespondierende in $\{(x,q)\}$ beginnende Lauf in $M'_{(x,q)}$. Da (x,q) nicht periodisch ist, gilt für alle ergodischen Mengen von $M'_{(x,q)}$, daß diese keinen Zustand enthalten, der (x,q) enthält. Nun gilt aber mit Wahrscheinlichkeit 1, daß Y'' in einer ergodischen Menge von $M'_{(x,q)}$ endet (und somit darin verbleibt)[15]. Also gilt mit Wahrscheinlichkeit 1, daß es nur endlich viele Indizes $i_1, i_2, \ldots, i_k$ gibt, mit

[14] zur Erklärung siehe [Bau78]
[15] siehe Abschnitt 1.3.2, Seite 21

$(x,q) \in Y_{i_j}$. Sei nun $Y' = \widehat{Y}_0, \widehat{Y}_1, \widehat{Y}_2, \ldots$ ein zu Y korrespondierender Lauf in $\mathcal{T}_{prob} \times \mathcal{A}$ mit $\widehat{Y}_0 = (x,q)$. Dann gilt aufgrund der Potenzmengenkonstruktion, daß $\widehat{Y}_i \in Y_i,\ i = 0,1,2,\ldots$. Falls also $\widehat{Y}_j = (x,q)$ dann folgt daraus, daß $j \in \{i_1, i_2, \ldots, i_k\}$. Somit gibt es mit Wahrscheinlichkeit 1 nur endlich viele Indizes mit $\widehat{Y}_i = (x,q)$. Das Ereignis $\mathbf{Wdh}_2$ tritt also mit Wahrscheinlichkeit 0 ein.

- $(x_{start}, q_{start}) \neq (x_{wdh}, q_{wdh}) = (x,q)$
  Sei $\mathbf{Wdh}_2^i$ das Ereignis, daß ein in x_{start} beginnender Lauf Y von $\mathcal{T}_{prob}$ zu einem Lauf $Y' = y_0, y_1, y_2, \ldots$ von $\mathcal{T}_{prob} \times \mathcal{A}$ korrespondiert, mit Y' beginnt in (x_{start}, q_{start}), durchläuft (x_{wdh}, q_{wdh}) unendlich oft und es gilt :

  - $y_i = (x_{wdh}, q_{wdh})$
  - $y_j \neq (x_{wdh}, q_{wdh}),\ j < i.$

  Dann gilt

  $$\{Y | Y \text{ erfüllt } \mathbf{Wdh}_2\} \ = \ \cup_{i \in \mathbb{N}} \{Y | Y \text{ erfüllt } \mathbf{Wdh}_2^i\}.$$

  Nun ist aber $\forall i \in \mathbb{N}$ die Wahrscheinlichkeit für das Ereignis $\mathbf{Wdh}_2^i$ gleich $0.^{(*)}$ Da auf der rechten Seite der obigen Gleichung eine abzählbare Vereinigung steht, folgt, daß Ereignis $\mathbf{Wdh}_2$ mit Wahrscheinlichkeit 0 eintritt.

  Zu $^{(*)}$: Sei $i \in \mathbb{N}$. Sei $\mathbf{A_i} = \{Y | Y \text{ erfüllt } \mathbf{Wdh}_2^i\}$. Sei

  $$\mathbf{B} = \{Y \mid Y \text{ erfüllt } \mathbf{Wdh}_2 \text{ mit } (x_{start}, q_{start}) = (x_{wdh}, q_{wdh}) = (x,q)\}.$$

  Dann wissen wir, daß $\mathbf{B}$ Mass 0 hat.

  Es gilt

  $$\mathbf{A_i} \ \subset \ \cup_{x_0,\ldots,x_{i-1} \in X} \Delta(x_0, \ldots, x_{i-1})\mathbf{B}.$$

  Aufgrund der Markov Eigenschaft gilt

  $$\mu(\Delta(x_0, \ldots, x_{i-1})\mathbf{B}) \ = \ \mu(\Delta(x_0, \ldots, x_{i-1})) \cdot \mu(\mathbf{B}) \ = \ 0.$$

  Also folgt $\mu(\mathbf{A_i}) \ = \ 0.$

□

Wir haben nun alles beisammen, um den gewünschten Wert

$$\mu(\mathbf{Y}_{\models \mathcal{A}})$$

zu bestimmen. Ähnlich wie die Markov Kette $M'_{(x,q)}$ definieren wir jetzt basierend auf dem zugrundeliegenden Graphen von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$ eine Markovkette.

Definition 2.2.8. [**Die Markov Kette M'_{sdet}]**
Sei $G = (Q'', E)$ der zugrundeliegende Graph von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$. Sei Q''_0 die Menge der Startzustände von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$. Dann definieren wir M'_{sdet} als

$$M'_{sdet} \;=\; (Q'', E, \tilde{p}, \tilde{p}_0),$$

wobei

- $\tilde{p}((x,R),(x',R')) \;=\; p_{xx'}$ für $((x,R),(x',R')) \in E$.
- $\tilde{p}_0((x,R)) \;=\; p_0(x), \quad (x,R) \in Q''_0$.

Dann ist M'_{sdet} eine endliche Markov Kette. Wir bezeichnen mit μ'_{sdet} das Wahrscheinlichkeitsmaß des Folgenraums von M'_{sdet}. ■

Als nächstes machen wir eine Aussage über den Zusammenhang der Wahrscheinlichkeitsräume von M und M'_{sdet}.

Definition 2.2.9. [**Die Projektion π]**
Sei π folgende Abbildung zwischen den Läufen von M'_{sdet} und den Läufen von M.

$$\pi \;:\; (Q'')^{\omega} \;\longrightarrow\; X^{\omega}$$

$$(x_0,R_0),(x_1,R_1),(x_2,R_2),\ldots \;\longmapsto\; x_0,x_1,x_2,\ldots$$

Für eine Menge $A \subset (Q'')^{\omega}$ definieren wir

$$\pi(A) \;=\; \{\pi(Y) \mid Y \in A\}.$$

Bemerke, daß wir π auch auf endliche Wörter über Q'' anwenden werden. Wir meinen dann die offensichtliche Abbildung $\pi : \cup_{k\in\mathbb{N}}(Q'')^k \to \cup_{k\in\mathbb{N}}X^k$.

■

Dann ist π meßbar, da

$$\pi^{-1}(\Delta(x_0,x_1,\ldots,x_n)) \;=\; \bigcup_{(x_0,R_0),\ldots,(x_n,R_n)\in Q''} \Delta'((x_0,R_0),(x_1,R_1),\ldots,(x_n,R_n)).^{16}$$

[16] Wobei mit $\Delta'(.)$ die Basiszylinder von M'_{sdet} gemeint sind.

Lemma 2.4. *Sei* $\mathbf{Y}$ *meßbar in* M*. Dann gilt*

$$\mu(\mathbf{Y}) \;=\; \mu'_{sdet}(\pi^{-1}(\mathbf{Y})).$$

Beweis : Sei $\tilde{\mu}$ das Bildmaß von μ'_{sdet} unter π, d. h.

$$\tilde{\mu}(\mathbf{Y}) \;=\; \mu'_{sdet}(\pi^{-1}(\mathbf{Y})) \text{ für alle } \mathbf{Y} \text{ meßbar in } M.$$

Dann ist $\tilde{\mu}$ ein Wahrscheinlichkeitsmaß auf der σ-Algebra Δ des Folgenraums von M, und $\tilde{\mu}$ stimmt mit μ auf den Basiszylindern von M überein. Da aufgrund der Schnittstabilität der Basiszylinder die Fortsetzung von μ auf Δ eindeutig ist, folgt

$$\tilde{\mu} \;=\; \mu,$$

was die Behauptung des Lemmas ist.

□

Wir können also nun die Markov Kette M'_{sdet} benutzen, um die gewünschte Wahrscheinlichkeit $\mu(\mathbf{Y}_{\models\mathcal{A}})$ zu berechnen. Dazu unterteilen wir noch die ergodischen Mengen von M'_{sdet} in zwei Klassen ein.

Definition 2.2.10. [**Akzeptierende ergodische Mengen]**
Wir nennen eine ergodische Menge C von M'_{sdet} *akzeptierend,* falls C einen Zustand enthält, der einen periodischen Zustand von $T_{prob} \times \mathcal{A}$ enthält, dessen zweite Komponente ein Akzeptanzzustand von $\mathcal{A}$ ist. Also C ist akzeptierend, falls gilt:

$$\exists (x, q_F) \text{ periodisch und } (x,R) \in C \text{ mit } (x,q_F) \in (x,R) \;\wedge\; q_F \in F.$$

Ansonsten nennen wir *C nicht akzeptierend.* ■

Satz 2.2.

$$\mu(\mathbf{Y}_{\models\mathcal{A}})$$

ist gleich der Wahrscheinlichkeit, daß ein Lauf von M'_{sdet} *in einer akzeptierenden ergodischen Menge von* M'_{sdet} *endet.*

Beweis : Sei *Fair* die Menge aller Läufe in M'_{sdet}, die in einer ergodischen Menge von M'_{sdet} enden und jeden Zustand dieser Menge unendlich oft durchlaufen. Wir wissen aus Abschnitt 1.3.2, Seite 21, daß $\mu'_{sdet}(Fair) = 1$.

Sei $Fair_{akz} \subset Fair$ die Menge der Läufe in *Fair,* die in einer akzeptierenden ergodischen Menge von M'_{sdet} enden.

Sei $Fair_{\neg akz} \subset Fair$ die Menge der Läufe in $Fair$, die in einer nicht akzeptierenden ergodischen Menge von M'_{sdet} enden. Dann gilt

$$\mu(\mathbf{Y}_{\models\mathcal{A}})$$

$= ^{17} \mu(\mathbf{Y}'_{\models\mathcal{A}})$
$= \mu'_{sdet}(\pi^{-1}(\mathbf{Y}'_{\models\mathcal{A}}))$
$= \mu'_{sdet}(\pi^{-1}(\mathbf{Y}'_{\models\mathcal{A}}) \cap Fair)$
$= ^{18} \mu'_{sdet}((\pi^{-1}(\mathbf{Y}'_{\models\mathcal{A}}) \cap Fair_{akz}) \bigcup (\pi^{-1}(\mathbf{Y}'_{\models\mathcal{A}}) \cap Fair_{\neg akz}))$
$= \mu'_{sdet}(\pi^{-1}(\mathbf{Y}'_{\models\mathcal{A}}) \cap Fair_{akz}) + \mu'_{sdet}(\pi^{-1}(\mathbf{Y}'_{\models\mathcal{A}}) \cap Fair_{\neg akz})$

Wir zeigen nun, daß

$$\mu'_{sdet}(\pi^{-1}(\mathbf{Y}'_{\models\mathcal{A}}) \cap Fair_{akz}) = \mu'_{sdet}(Fair_{akz})$$

und

$$\mu'_{sdet}(\pi^{-1}(\mathbf{Y}'_{\models\mathcal{A}}) \cap Fair_{\neg akz}) = 0.$$

Dann gilt also

$$\mu(\mathbf{Y}_{\models\mathcal{A}}) = \mu'_{sdet}(Fair_{akz}),$$

was die Aussage des Lemmas beweist.[19]

- Z. z. $\mu'_{sdet}(\pi^{-1}(\mathbf{Y}'_{\models\mathcal{A}}) \cap Fair_{akz}) = \mu'_{sdet}(Fair_{akz})$.
  Z. z. ist also, daß für ein $Y'' \in Fair_{akz}$ gilt, daß $\pi(Y'')$ mit Wahrscheinlichkeit 1 von $\mathcal{A}$ akzeptiert wird. Bemerke, daß $\pi(Y'')$ ein echter Lauf von M ist (siehe Konstruktion von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$). Somit wird also aufgrund des Lemmas 2.1, Seite 41, $\pi(Y'')$ genau dann von $\mathcal{A}$ akzeptiert, wenn es einen akzeptierenden Lauf in $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ gibt, der zu $\pi(Y'')$ korrespondiert.

  Es genügt somit zu zeigen, daß für ein $Y'' \in Fair_{akz}$ gilt, daß es mit Wahrscheinlichkeit 1 einen zu $\pi(Y'')$ korrespondierenden akzeptierenden Lauf in $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ gibt.

[17] siehe Gleichung 2.1, Seite 42

[18] dies ist eine disjunkte Vereinigung

[19] Bemerke, daß die Läufe von M'_{sdet}, die in einer akzeptierenden ergodischen Menge von M'_{sdet} enden, aber nicht jeden Zustand dieser ergodischen Menge unendlich oft durchlaufen, eine Nullmeng bezüglich μ'_{sdet} darstellen.

Sei $Y'' = X_0, X_1, X_2, \ldots$ ein Lauf in $Fair_{akz}$. Sei C eine akzeptierende ergodische Menge von M'_{sdet} und $k \in \mathbb{N}$ so, daß

$$X_j \in C, \quad \forall j \geq k$$

gilt. Da C akzeptierend ist, gibt es (x_F, q_F) periodisch und einen Zustand $y \in C$ mit

$$(x_F, q_F) \in y.$$

Sei $\gamma_{(x_F,q_F)}$ das mit (x_F, q_F) assoziierte endliche Wort über X aus Definition 2.2.4, Seite 43. Da nun mit Wahrscheinlichkeit 1 gilt, daß Y'' jeden Zustand von C unendlich oft durchläuft (siehe Abschnitt 1.3.2, Seite 21) kann man wie im Beweis von Lemma 2.2, Seite 44, zeigen, daß es mit Wahrscheinlichkeit 1 ein $d \in \mathbb{N}$ gibt, so daß gilt:

$$X_d = y, \qquad \pi(X_{d+1} \cdots X_{d+|\gamma_{(x_F,q_F)}|}) = \gamma_{(x_F,q_F)}.$$

Nun gilt mit Lemma 2.2, Seite 44, daß $\pi(X_d, X_{d+1}, X_{d+2}, \ldots)$ mit Wahrscheinlichkeit 1 zu einem Lauf $Y' = (x_d, q_d), (x_{d+1}, q_{d+1}), \ldots$ von $\mathcal{T}_{prob} \times \mathcal{A}$ korrespondiert, mit Y' beginnt in (x_F, q_F) und durchläuft (x_F, q_F) unendlich oft. Wir haben also, daß mit Wahrscheinlichkeit 1 gilt:

- $X_d = y = (x_F, R)$ und
- $\pi(X_d), \pi(X_{d+1}), \pi(X_{d+2}), \ldots$ korrespondiert zu einem Lauf $Y' = (x_d, q_d), (x_{d+1}, q_{d+1}), \ldots$ von $\mathcal{T}_{prob} \times \mathcal{A}$, mit Y' beginnt in (x_F, q_F) und durchläuft (x_F, q_F) unendlich oft.

Falls aber die beiden Eigenschaften gegeben sind, folgt leicht, daß $\pi(Y'') = \pi(X_0, X_1, \ldots)$ zu einem akzeptierenden Lauf von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ korrespondiert, was das Lemma beweist.

Hierzu müssen wir nur noch zeigen, daß das Anfangsstück $\pi(X_0, X_1, \ldots, X_d)$ zu einem endlich Lauf von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ korrespondiert, der in einem Anfangszustand von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ beginnt und im Zustand (x_F, q_F) endet. Dies folgt induktiv (vgl. Bemerkung 5, Seite 41) wie folgt:

es gilt $(x_F, q_F) \in X_d$
$\Rightarrow$ $\exists\, (x_{d-1}, q_{d-1}) \in X_{d-1}$ mit $(x_F, q_F) \in \rho((x_{d-1}, q_{d-1}), x_F)$[20]
$\Rightarrow$ $\exists\, (x_{d-2}, q_{d-2}) \in X_{d-2}$ mit $(x_{d-1}, q_{d-1}) \in \rho((x_{d-2}, q_{d-2}), x_{d-1})$

[20] ρ war die Übergangsfunktion von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$.

$\vdots$

$\Rightarrow \quad \exists\, (x_0,q_0) \in X_0$ mit $(x_1,q_1) \in \rho((x_0,q_0),x_1)$

Da alle Elemente von X_0 Startzustände von $(\mathcal{T}_{prob} \times \mathcal{A})$ sind[21], leistet die Sequenz $(x_0,q_0),(x_1,q_1),\ldots,(x_{d-1},q_{d-1}),(x_F,q_F)$ das gewünschte.

- Z. z. $\mu'_{sdet}(\pi^{-1}(\mathbf{Y}'_{\models\mathcal{A}}) \cap Fair_{\neg akz}) = 0$.

  Z. z. ist also, daß für ein $Y'' \in Fair_{\neg akz}$ gilt, daß $\pi(Y'')$ mit Wahrscheinlichkeit 0 von $\mathcal{A}$ akzeptiert wird. Bemerke, daß $\pi(Y'')$ ein echter Lauf von M ist (siehe Konstruktion von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$). Somit wird also aufgrund des Lemmas 2.1, Seite 41, $\pi(Y'')$ genau dann von $\mathcal{A}$ akzeptiert, wenn es einen akzeptierenden Lauf in $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ gibt, der zu $\pi(Y'')$ korrespondiert.

  Es genügt somit zu zeigen, daß für ein $Y'' \in Fair_{\neg akz}$ gilt, daß es mit Wahrscheinlichkeit 0 einen zu $\pi(Y'')$ korrespondierenden akzeptierenden Lauf in $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ gibt.

  Dies folgt sofort aus Lemma 2.3, Seite 47. Angenommen,

  $$Y'' = (x_0,R_0),(x_1,R_1),(x_2,R_2),\ldots$$

  ist ein Lauf in $Fair_{\neg akz}$. Dann gilt, daß Y'' in einer nicht akzeptierenden ergodischen Menge C endet. Es gibt also einen Index $k \in \mathbb{N}$, mit

  $$(x_j,R_j) \in C, \quad j \geq k.$$

  Wir wissen, daß für jeden zu $\pi(Y'') = x_0,x_1,x_2,\ldots$ korrespondierenden Lauf $y_0,y_1,y_2,\ldots$ von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ aufgrund der Konstruktion von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ und $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$ gilt, daß

  $$y_i \in (x_i,R_i), \quad i \geq 0.$$

  Fall es nun unendliche viele Indizes $i_1,i_2,\ldots$ gibt, mit

  $$y_{i_1} = y_{i_2} = y_{i_3} = \ldots\ ,$$

  so gibt es einen Index $i_l > k$, also gilt

  $$y_{i_1} = y_{i_l} \in (x_l,R_l) \in C.$$

[21] siehe Definition 2.2.8 von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$, Seite 49 und die Definition 2.1.2 der Potenzmengenkonstruktion, Seite 29

Da C nicht akzeptierend ist, folgt, daß y_{i_1} nicht periodisch ist. Somit folgt mit Lemma 2.3, Seite 47 (mit (x_{start}, q_{start}) beliebig und $(x_{wdh}, q_{wdh}) = y_{i_1}$), daß die Wahrscheinlichkeit für einen solchen zu $\pi(Y'') = x_0, x_1, x_2, \ldots$ korrespondierenden Lauf $y_0, y_1, y_2, \ldots$ von $(\mathcal{T}_{prob} \times \mathcal{A})_{NBA}$ gleich 0 ist. Dies gilt insbesondere für $y_{i_1} \in Q \times F$.

□

Mit Satz 2.2 haben wir nun das richtige Werkzeug, um den Wert $\mu(\mathbf{Y}_{\models \mathcal{A}})$ algorithmisch berechnen zu können. Wir geben folgenden Algorithmus an:

Algorithmus 1 Grundidee eines quantitativen probabilistischen Modelchecking Algorithmus mit *Buechi*-Automaten

---

- Eingabe : gegeben sei ein Probabilistisches Programm $\mathcal{T}'_{prob} = (M, AP, L')$ und eine LTL-Formel φ über AP
- Ausgabe : ausgegeben wird der Wert $\mu(\mathbf{Y}_{\models \varphi})$

---

1. Erstelle NBA $\mathcal{A}' = (Q', AP, \delta', Q_0, F)$ mit $\mathcal{L}_\omega(\mathcal{A}') = \mathcal{L}_\omega(\varphi)$.
2. Verändere $\mathcal{A}'$ und $\mathcal{T}'_{prob}$ gemäß den Bemerkungen und Vereinfachungen von Seite 36. Sei $\mathcal{A} = (Q, X, \delta, \{q_0\}, F)$ der so aus $\mathcal{A}'$ enstandene NBA und $\mathcal{T}_{prob} = (M, X, L)$ das aus $\mathcal{T}'_{prob}$ enstandene Probabilistische Programm.
3. Konstruiere den Automaten $\mathcal{T}_{prob} \times \mathcal{A}$.
4. Berechne die Menge der periodischen Zustände (x, q) von $T_{prob} \times \mathcal{A}$ mit $q \in F$.
5. Konstruiere die Markov Kette M'_{sdet}.
6. Berechne den Wert $\mu(\mathbf{Y}_{\models \varphi})$ gemäß Satz 2.2, Seite 50.

Bevor wir nun auf die einzelnen Schritte des Algorithmus eingehen, bemerken wir noch folgende Punkte :

- Wir können die gleiche Vorgehensweise benutzen, wenn wir eine Spezifikation haben, die durch einen NBA gegeben ist (für einen NBA $\mathcal{A}$ gilt: $\mathcal{L}_\omega(\mathcal{A})$ ist messbar im Folgenraum einer Markov Kette (siehe [Va85])). In diesem Fall fällt also nur Schritt 1 des Algorithmus weg.

- Desweiteren bemerken wir, daß gilt :

$$\mu(\mathbf{Y}_{\models\varphi}) = 1 \iff$$

alle erreichbaren ergodischen Mengen von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$ sind akzeptierend.
Somit können wir für qualitatives LTL-Model Checking einige Schritte des Algorithmus vereinfachen. In Schritt 5 brauchen wir z. B. nicht die exakten Wahrscheinlichkeiten von M'_{sdet} betrachten, sondern nur den zugrundeliegenden Graphen. Anstelle von Schritt 6 überprüfen wir dann, ob alle erreichbaren ergodischen Mengen von $(\mathcal{T}_{prob} \times \mathcal{A})_{sdet}$ akzeptierend sind.

Definition 2.2.11.
Sei A eine Teilmenge der Zustände von $\mathcal{T}_{prob} \times \mathcal{A}$ und $(x,q) \in A$. Wir bezeichnen mit

$$A_{det}((x,q))$$

denjenigen deterministischen Automaten, den man erhält, indem man die Potenzmengenkonstruktion nur auf die Zustände in A anwendet. Zudem betrachten wir nur den vom Zustand $\{(x,q)\}$ erreichbaren Teil und definieren $\{(x,q)\}$ als Anfangszustand von $A_{det}((x,q))$. Auch hier besteht ein erreichbarer Zustand nur aus Zuständen von $\mathcal{T}_{prob} \times \mathcal{A}$, die dieselbe erste Komponente besitzen. ■

Bevor wir nun fortfahren, wollen wir uns überlegen, welche Struktur der zugrundeliegende Graph von $C_{det}((x,q))$ im Vergleich zum zugrundeliegenden Graphen von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ besitzt, falls C eine starke Zusammenhangskomponente (SCC) von $\mathcal{T}_{prob} \times \mathcal{A}$ ist und $(x,q) \in C$ gilt. Dies werden wir dann später benötigen. Dazu noch eine Definition.

Definition 2.2.12. [Der Graph $^{G}/_{\tau}$.]
Sei $G = (V,E)$ ein gerichteter Graph und $\tau = \{V_1,\ldots,V_k\}$ eine Partition von V, d. h.

$$\cup_{i=1,\ldots,k} V_i \;=\; V \quad \wedge \quad V_i \cap V_j \;=\; \emptyset,\;\; i \neq j.$$

Dann bezeichnen wir mit $^{G}/_{\tau}$ den gerichteten Graphen (V',E') mit

- $V' = \{V_1,\ldots,V_k\} = \tau$
- $(V_i,V_i) \in E' \quad \Leftrightarrow \quad \exists v \in V_i \wedge v' \in V_j \mid (v,v') \in E$

■

Sei im folgenden

$$G = (V, E)$$

der zugrundeliegende Graph von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$.

Lemma 2.5. *Sei C eine starke Zusammenhangskomponente von $\mathcal{T}_{prob} \times \mathcal{A}$ und $(x,q) \in C$. Sei*

$$V' \;=\; \{v \in V \;:\; v \cap C \neq \emptyset\}.$$

Sei G' der von V' induzierte Teilgraph von G. Sei

$$\widetilde{V} \;=\; \{v \cap C \;:\; v \in V'\}$$

und

$$\tau \;=\; \{\{v \in V' \;:\; v \cap C = v'\} \mid v' \in \widetilde{V}\}.$$

τ ist also eine Partition der Zustände in V' bezüglich ihrer C-Anteile. Sei

$$\widetilde{G} \;=\; {}^{G'}\!/_{\tau}.$$

Dann ist $\widetilde{G} = (\tau, \widetilde{E})$ isomorph zum zugrundeliegenden Graphen von $C_{det}((x,q))$, und ein Isomorphismus der Knoten ist gegeben durch

$$\tau \ni s \quad \overset{f}{\longmapsto} \quad v \cap C, \;\; \textit{mit } v \textit{ beliebig aus } s.$$

Dies bedeutet nichts anderes, als daß man den zugrundeliegenden Graphen von $C_{det}((x,q))$ aus dem zugrundeliegenden Graphen von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ erhält, indem man erst alle Knoten entfernt, die kein Element aus C enthalten und dann aus den übrig gebliebenen Knoten die Elemente entfernt, die nicht in C liegen. Zum Schluss muss man dann noch alle die Knoten verschmelzen, die den gleichen C-Anteil hatten.

Beweis : Wir zeigen, daß die Abbildung f eine Bijektion zwischen τ und den Knoten von $C_{det}((x,q))$ ist.

- f ist wohldefiniert : Sei $s \in \tau$. Z. z.:
  - $v \cap C = v' \cap C, \quad v, v' \in s$.
    Dies ist offensichtlich, da τ die Zustände in V' gerade bezüglich ihrer C-Anteile partitioniert.

– $f(s)$ ist Knoten von $C_{det}((x,q))$.
Es ist a priori nicht ersichtlich, daß $f(s)$ ein Zustand von $C_{det}((x,q))$ ist. Da aber $s \in \tau$, folgt $\emptyset \neq s \subset V'$ mit

$$\forall v, v' \in s \; : \; v \cap C \; = \; v' \cap C \; \neq \; \emptyset.$$

Sei nun $v \in s$. v ist also ein Zustand in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$. Es gibt somit einen Pfad

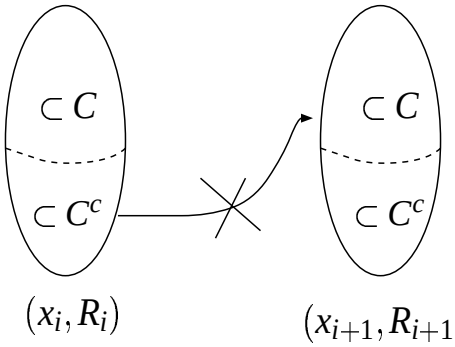
$$\{(x,q)\}, (x_1, R_1), \ldots, (x_n, R_n), v$$

von $\{(x,q)\}$ nach v im zugrundeliegenden Graphen von

$$(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q)).$$

Wir können jetzt induktiv zeigen, daß $(x_i, R_i) \cap C$, $i = 1, 2, \ldots, (n+1)$ mit $(x_{n+1}, R_{n+1}) = v$ ein Zustand in $C_{det}((x,q))$ ist.

* Induktionsanfang : $i = 1$
Da $\{(x,q)\}$ eine Teilmenge von C ist, ist die Behauptung offensichtlich.
* Induktionsschritt : $(x_i, R_i) \cap C$ sei ein Zustand von $C_{det}((x,q))$ und es gelte $i < (n+1)$. Dann folgt die Behauptung aus der Tatsache, daß es für ein $(x_i, q_i) \in (x_i, R_i) \setminus C$ in $\mathcal{T}_{prob} \times \mathcal{A}$ keinen Übergang zu einem Zustand $(x_{i+1}, q_{i+1}) \in (x_{i+1}, R_{i+1}) \cap C$ gibt.



Gäbe es ein solches (x_i, q_i), dann wissen wir mit Bemerkung 5 ,Seite 41, daß es im zugrundeliegenden Graph von $\mathcal{T}_{prob} \times \mathcal{A}$ einen Pfad

$$(x,q), (x_1, q_1), \ldots, (x_i, q_i)$$

gäbe, also auch den Pfad

$$(x,q), (x_1, q_1), \ldots, (x_i, q_i), (x_{i+1}, q_{i+1}).$$

Das wäre aber ein Widerspruch dazu, daß (x,q) und (x_{i+1},q_{i+1}) beide in der selben starken Zusammenhangskomponente C liegen und (x_i,q_i) nicht in C liegt. Somit kann es einen solchen Übergang in $\mathcal{T}_{prob}\times\mathcal{A}$ nicht geben. D. h. , daß es für jeden Zustand $b\in(x_{i+1},R_{i+1})\cap C$ einen Zustand $a\in(x_i,R_i)\cap C$ gibt, mit $\mathcal{T}_{prob}\times\mathcal{A}$ hat einen x_{i+1}-Übergang von a nach b. Da $(x_i,R_i)\cap C$ nach Induktionsvoraussetzung ein Zustand von $C_{det}((x,q))$ ist, folgt dies auch für $(x_{i+1},R_{i+1})\cap C = v\cap C = f(s)$.

- f ist surjektiv : Sei (x',R') ein Zustand in $C_{det}((x,q))$. Dann gibt es im zugrundeliegenden Graphen von $C_{det}((x,q))$ einen Pfad

$$\{(x,q)\},(x_1,R'_1),\ldots,(x_n,R'_n),(x',R').$$

Sei

$$\{(x,q)\},(x_1,R_1),\ldots,(x_n,R_n),(x',R)$$

der durch die ersten Komponenten eindeutig definierte Pfad im zugrundeliegenden Graphen von $(\mathcal{T}_{prob}\times\mathcal{A})_{det}((x,q))$. Offensichtlich gilt

$$(x_i,R'_i)\subset(x_i,R_i)\cap C \quad\wedge\quad (x',R')\subset(x',R)\cap C.$$

Wir wollen nun die umgekehrte Inklusion

$$(x_i,R'_i)\supset(x_i,R_i)\cap C \quad\wedge\quad (x',R')\supset(x',R)\cap C$$

zeigen. Dies folgt aber wiederum induktiv aus der Tatsache, daß es für ein $(x_i,q_i)\in(x_i,R_i)\setminus C$ in $\mathcal{T}_{prob}\times\mathcal{A}$ keinen Übergang zu einem Zustand $(x_{i+1},q_{i+1})\in(x_{i+1},R_{i+1})\cap C$ gibt. Sei $x_{n+1}=x'$, $R_{n+1}=R$, $R'_{n+1}=R'$.

  - Induktionsanfang : $i=1$
    Da $\{(x,q)\}$ eine Teilmenge von C ist, ist die Behauptung offensichtlich.
  - Induktionsschritt : Es gelte $(x_i,R'_i)\supset(x_i,R_i)\cap C$ und $i<(n+1)$. Da es nun für jeden Zustand $b\in(x_{i+1},R_{i+1})\cap C$ einen Zustand $a\in(x_i,R_i)\cap C$ gibt, mit $\mathcal{T}_{prob}\times\mathcal{A}$ hat einen x_{i+1}-Übergang von a nach b, folgt $(x_{i+1},R'_{i+1})\supset(x_{i+1},R_{i+1})\cap C$.

Es gilt also

$$(x',R')=(x',R)\cap C\neq\emptyset.$$

Damit gibt es ein $s \in \tau$ mit $(x',R) \in s$. Für dieses s gilt offensichtlich

$$f(s) = (x',R) \cap C = (x',R'),$$

was die Surjektivität von f beweist.

- f ist injektiv : Dies ist trivial, da τ die Menge V' nach dem C-Anteil ihrer Elemente partitioniert und f ein Element von τ gerade auf seinen C-Anteil abbildet.

Sei $\widehat{G} = (\widehat{V}, \widehat{E})$ der zugrundeliegende Graph von $C_{det}((x,q))$. Somit haben wir gezeigt, daß f eine Bijektion zwischen der Menge der Knoten von $\widetilde{G}$ und der Menge der Knoten von $\widehat{G}$ ist. Es bleibt also noch zu zeigen, daß τ verträglich ist mit den Kantenmengen von $\widetilde{G}$ und $\widehat{G}$, daß also gilt :

$$\forall s,t \in \tau \; : \; (s,t) \in \widetilde{E} \iff (f(s), f(t)) \in \widehat{E}.$$

Seien $s,t \in \tau$.
"$\Longrightarrow$: " Es gelte $(s,t) \in \widetilde{E}$. Es gibt also $(x',R') \in s, (x'',R'') \in t$, so daß es für alle $b \in (x'',R'')$ ein $a \in (x',R')$ gibt, so daß gilt: es gibt einen x''-Übergang von a nach b in $\mathcal{T}_{prob} \times \mathcal{A}$. Wiederum gilt, daß es für ein $a \in (x',R') \setminus C$ in $\mathcal{T}_{prob} \times \mathcal{A}$ keinen Übergang zu einem Zustand $b \in (x'',R'') \cap C$ gibt. Somit gibt es für alle $b \in (x'',R'') \cap C$ ein $a \in (x',R') \cap C$, so daß gilt: es gibt einen x''-Übergang von a nach b in $\mathcal{T}_{prob} \times \mathcal{A}$. Da $f(s) = (x',R') \cap C$ und $f(t) = (x'',R'') \cap C$ folgt $(f(s), f(t)) \in \widehat{E}$.
"$\Longleftarrow$: " Es gelte $(f(s), f(t)) \in \widehat{E}$. Sei nun $(x',R') \in s$ beliebig. Also gilt: $(x',R') \cap C = f(s)$. Sei

$$t = \{(x'',R''_1), \ldots, (x'',R''_k)\}.$$

Da es nun in $\mathcal{T}_{prob} \times \mathcal{A}$ keine x''-Übergänge von Elementen aus $(x',R') \setminus C$ nach $(x'',R''_i) \cap C$ gibt, folgt, daß es in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ einen x''-Übergang von (x',R') zu einem Zustand u gibt, mit $u \cap C = f(t)$. Dann folgt aber $u \in t$ und somit gilt auch $(s,t) \in \widetilde{E}$.

□

Es gilt also, daß $\widetilde{G} = (\tau, \widetilde{E})$ isomorph zum zugrundeliegenden Graphen von $C_{det}((x,q))$ ist. Diesen Sachverhalt werden wir im nächsten Lemma benötigen, in dem wir zeigen werden, daß in einer starken Zusammenhangskomponente (SCC) von $\mathcal{T}_{prob} \times \mathcal{A}$ entweder alle Zustände periodisch sind, oder keiner. Ausserdem zeigen wir, daß man für eine SCC C von $\mathcal{T}_{prob} \times \mathcal{A}$ nur $C_{det}((x,q)),\ (x,q) \in C$ und nicht ganz $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ betrachten muss, um zu entscheiden, ob die

Zustände von C periodisch sind oder nicht. Dies wird die Berechnung der periodischen Zustände von $\mathcal{T}_{prob} \times \mathcal{A}$ in Schritt 4 des Algorithmus erheblich vereinfachen. Dafür zuvor noch folgende Definition.

Definition 2.2.13. **[völlig spezifiziert]**
Sei A eine Teilmenge der Zustände von $\mathcal{T}_{prob} \times \mathcal{A}$. Sei $(x,q) \in A$ ein Zustand in A. Sei (x',R') ein Zustand in $A_{det}((x,q))$. Wir nennen (x',R') *völlig spezifiziert* in $A_{det}((x,q)$, falls für alle Transitionen (x',x'') in $\mathcal{T}$ gilt, daß (x',R') einen Übergang auf dem Buchstaben x'' in $A_{det}((x,q))$ hat. (x',R') ist also völlig spezifiziert, genau dann, wenn gilt:

$$\forall (x',x'') \in T \text{ gilt : } \exists (x'',R'') \text{ Zustand von } A_{det}((x,q) \text{ mit } ((x',R'),(x'',R''))$$

ist eine Kante im zugrundeliegenden Graphen von $A_{det}((x,q)$.

■

Bemerke, daß zwar jeder Zustand von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ völlig spezifiziert[22] ist in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$, jedoch ist i. Allg. nicht jeder Zustand von $A_{det}((x,q))$ in $A_{det}((x,q))$ völlig spezifiziert.

Lemma 2.6. *Sei C eine starke Zusammenhangskomponente (SCC) von $\mathcal{T}_{prob} \times \mathcal{A}$ und $(x,q) \in C$ ein Zustand in C. Folgende Aussagen sind dann äquivalent:*

1. *(x,q) ist periodisch.*

2. *Es gibt eine ergodische Menge D' von $C_{det}((x,q))$ für die gilt:*

   $$y \text{ ist völlig spezifiziert } \forall y \in D'.$$

3. *Es gibt im zugrundeliegenden Graphen von M einen endlichen in x beginnenden Pfad $\gamma = x, x_1, \ldots, x_n$, so daß jeder Lauf von M, der γ als Präfix hat, einen korrespondieren, in (x,q) beginnenden Lauf von $\mathcal{T} \times \mathcal{A}$ besitzt, der nur Zustände von C durchläuft.*

4. *Alle Zustände in C sind periodisch.*

[22] Wir hatten vorausgesetzt, daß $\mathcal{A}$ in jedem Zustand für jeden Buchstaben aus X mindestens einen Übergang besitzt.

Beweis :
$1 \Rightarrow 2$: Sei (x,q) periodisch. Sei D eine ergodische Menge von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$, die einen Zustand (x,R) enthält, mit $(x,q) \in (x,R)$ (die Existenz einer solchen Menge folgt aus der Definition eines periodischen Zustands). Wir zeigen jetzt, daß gilt:

(a) Jeder Zustand auf einem Pfad von $\{(x,q)\}$ nach D enthält mindestens einen Zustand von C.

(b) Jeder Zustand von D enthält mindestens einen Zustand von C.

(c) Es gibt in $C_{det}((x,q))$ eine kanonische von D abgeleitete ergodische Menge D' von $C_{det}((x,q))$.

(d) Jeder Zustand von D' ist völlig spezifiziert in $C_{det}((x,q))$.

Dann ist 2 erfüllt.

Um die ersten beiden Punkte zu zeigen, bemerken wir folgendes: sei

$$circle = (x,q),(y_1,q_1),\ldots,(y_k,q_k),(x,q)$$

ein Kreis im zugrundeliegenden Graphen von $\mathcal{T}_{prob} \times \mathcal{A}$. Dann gilt: alle $(y_i,q_i), i = 1,\ldots,n$ liegen in der selben starken Zusammenhangskomponente wie (x,q)[23]. Es gilt also

$$(y_i,q_i) \in C \quad i = 1,2,\ldots,n.$$

Zu (a): Sei

$$\{(x,q)\},(y_1,R_1),\ldots,(y_n,R_n)$$

ein Pfad im zugrundeliegenden Graphen von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$, mit $(y_n,R_n) \in D$. Da nun (y_n,R_n) und (x,R) beide in der selben ergodischen Menge D liegen, gibt es einen Pfad

$$(y_n,R_n),(y_{n+1},R_{n+1}),\ldots,(x_{n+k},R_{n+k}),(x,R)$$

im zugrundeliegenden Graphen von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$. Somit ist

$$\{(x,q)\},(y_1,R_1),\ldots,(y_n,R_n),(y_{n+1},R_{n+1}),\ldots,(x_{n+k},R_{n+k}),(x,R)$$

[23]Bemerke, daß SCCs maximal sind bezüglich starkem Zusammenhang.

ein Pfad von $\{(x,q)\}$ nach (x,R). Da nun $(x,q) \in (x,R)$ gilt, wissen wir (vgl. Bemerkung 5, Seite 41), daß es in $\mathcal{T}_{prob} \times \mathcal{A}$ einen Kreis

$$circle = (x,q),(y_1,q_1),\ldots,(y_{n+k},q_{n+k}),(x,q)$$

gibt, mit $(y_i,q_i) \in (y_i,R_i),\ \ i = 1,2,\ldots,(n+k)$. Aus obiger Bemerkung folgt, daß $(y_i,q_i) \in C,\ \ i = 1,2,\ldots,(n+k)$. Somit enthält jeder Zustand auf dem Pfad von $\{(x,q)\}$ nach D mindestens einen Zustand von C, und (a) ist gezeigt.

Zu (b): Sei $(x',R') \in D$. Da D in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ erreichbar ist und D ergodisch, also insbesondere stark zusammenhängend ist, gibt es einen Pfad

$$\{(x,q)\},(y_1,R_1),\ldots,(y_n,R_n),(x',R')$$

im zugrundeliegenden Graphen von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$. Da (x',R') und (x,R) in der selben ergodischen Menge D liegen, kann man diesen Pfad folgendermassen verlängern:

$$\{(x,q)\},(y_1,R_1),\ldots,(y_n,R_n),(x',R'),(y_{n+2},R_{n+2}),\ldots,(y_{n+k},R_{n+k}),(x,R).$$

Mit der selben Argumentation wie in Teil (a) folgt aber nun, daß jeder Zustand dieses Pfades, also inbesondere auch (x',R') einen Zustand aus C enthält, was (b) zeigt.

Zu (c): Sei $D = \{s_1,\ldots,s_n\}$. Wir definieren

$$D' = \{s_i \cap C \mid i = 1,2,\ldots,n\}.$$

Bemerke, daß D' i. Allg. weniger Elemente enthält, als D. Es gilt: D' ist eine Teilmenge der Knoten des zugrundeliegenden Graphen von $C_{det}((x,q))$ (siehe Lemma 2.5, Seite 56 und bemerke, daß jeder Zustand von D mindestens einen Zustand von C enthält). Sei $\widehat{G} = (\widehat{V},\widehat{E})$ der zugrundeliegende Graph von $C_{det}((x,q))$.Wir zeigen, daß D' ergodische Menge von $\widehat{V}$ ist.

- Z. z.: D' ist erreichbar in $C_{det}((x,q))$.
  Da nach (a) jeder Zustand auf einem Pfad von $\{(x,q)\}$ nach D in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ mindestens einen Zustand von C enthält, folgt mit Lemma 2.5, daß D' in $C_{det}((x,q))$ erreichbar ist.

- Z. z.: D' ist stark zusammenhängend in $C_{det}((x,q))$.
  Der starke Zusammenhang von D' folgt auch sofort aus Lemma 2.5. Bemerke, daß nach (b) gilt, daß jeder Zustand von D mindestens einen Zustand aus

C enthält. Somit bleibt der von D induzierte Teilgraph erhalten, wenn man im zugrundeliegenden Graphen von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ die Knoten entfernt, die kein Element aus C enthalten und dann aus den übrig gebliebenen Knoten die Elemente entfernt, die nicht in C liegen. Wenn man zum Schluss dann noch alle die Knoten verschmilzt, die den gleichen C-Anteil hatten, so ändert dies natürlich am starken Zusammenhang nichts.

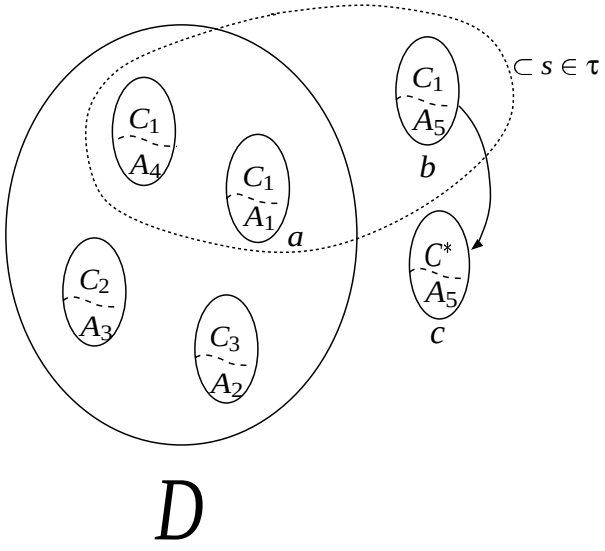
- Z. z.: D' ist abgeschlossen in $C_{det}((x,q))$,
  d. h. es führen in $\widehat{G}$ keine Kanten aus D' hinaus. Sei $u \in D'$ ein Zustand von $C_{det}((x,q))$. Mit den Bezeichnungen aus Lemma 2.5, Seite 56, sei $s \in \tau$ mit $f(s) = u$. Es gibt nun zwei Fälle:

  – $\forall a \in s \ : \ a \in D$. In diesem Fall führt offensichtlich keine Kante in $\widehat{G}$ von u aus D' hinaus. Dies folgt aus Lemma 2.5. Mit den Bezeichnungen aus Lemma 2.5 gilt nämlich, daß D ergodische Menge von G' ist (bemerke, daß nach (b) jeder Zustand von D nichtleeren Schnitt mit C hat). Da nun

  $$\widehat{G} \quad \text{isomorph zu} \quad {}^{G'}\!/_{\tau},$$

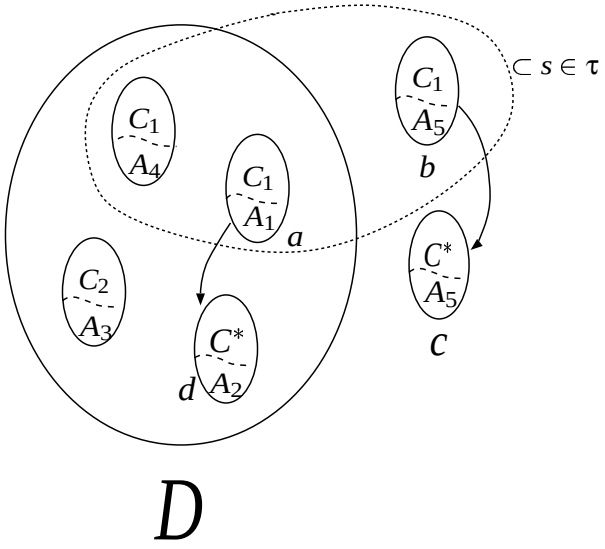
  folgt, daß in $\widehat{G}$ keine Kanten von u aus D' hinausführen.

  – $\exists a, b \in s \ : \ a \in D \ \wedge \ b \notin D$. Hier werden also bei der Bildung des Quotientengraphen ${}^{G'}\!/_{\tau}$ ein Zustand $\in D$ mit einem Zustand $\notin D$ identifiziert. Da D ergodisch, also auch abgeschlossen ist, führen die Kanten von u, die von Kanten von $a \in D$ abgeleitet werden, wieder nach D' hinein. Man könnte nun meinen, daß es jedoch Kanten von u gibt, die von Kanten von $b \notin D$ abgeleitet wurden und nicht mehr nach D' führen. Dies ist jedoch nicht der Fall, obwohl es natürlich Kanten in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ geben kann, die von b zu einem Zustand c führen, der nicht in D liegt. Das wollen wir jetzt zeigen. Nehmen wir also an, es gibt einen Zustand $c \notin D$, so daß es im zugrundeliegenden Graphen von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ eine Kante von b nach c gibt.



In der Grafik ist der Zustand $a = C_1 \cup A_1$, wobei $C_1 \subset C$ und $A_1 \cap C = \emptyset$ gelten soll. Entsprechendes gilt für die anderen Zustände. Angenommen, die Kante von b nach c repräsentiert einen x'-Übergang. Da $c \cap C \neq \emptyset$ (andernfalls wäre c kein Knoten in G' und unsere Bedenken wären hinlänglich) gilt und es auch gilt, daß es keinen Übergang von $b \setminus C$ nach $c \cap C$ geben kann, folgt: es gibt einen x'-Übergang von a aus. Da a aber in D liegt und D abgeschlossen ist, bedeutet dies, daß es einen Kante von a zu einem Zustand $d \in D$ gibt, die einen x'-Übergang repräsentiert. Nun gilt aber

$$d \cap C = c \cap C.$$



Also werden bei der Bildung des Quotientengraphen $\widehat{G}$ die Zustände c und d identifiziert. Da $d \in D$, werden c und d in $\widehat{G}$ durch einen Knoten in D' repräsentiert. Somit führt die Kante in $\widehat{G}$, die aus der Kante von b nach c (in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ entstanden ist, von einem Zustand in D', nämlich $f(s) = u$, zu einem Zustand in D', nämlich zu $f(v)$, wobei $v \in \tau$, so daß $d \in v$ gilt.

Da der dritte Fall $\forall a \in s : a \notin D$ nicht eintreten kann (bemerke: $f(s) = u \in D'$), haben wir damit gezeigt, daß für alle Kanten (u,v) von $\widehat{G}$ gilt: $v \in D'$. Da $u \in D'$ beliebig war, gilt also, daß D' abgeschlossen ist in $\widehat{G}$.

Zu (d): Wir zeigen jetzt noch, daß jeder Zustand von D' (aus (c)) völlig spezifiziert ist in $C_{det}((x,q))$. Sei u ein Zustand aus D'. Mit den Bezeichnungen aus Lemma 2.5, Seite 56, sei $s \in \tau$ mit $f(s) = u$. Dann gilt $s \cap D \neq \emptyset$. Sei $a \in s$. Dann wissen wir, daß a völlig spezifiziert ist in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$. [24] Sei nun $x' \in X$ beliebig. Es gibt also in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ einen x'-Übergang von a aus. Da $a \in D$, führt dieser x'-Übergang wieder nach D. Sei $b \in D$ der Zustand, in den $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ von a aus bei Eingabe x' wechselt. Da nach (b) jeder Zustand aus D einen nichtleeren Schnitt mit C besitzt, gibt es also ein $v \in D'$, so daß u einen x'-Übergang nach v besitzt. Da $u \in D'$ und $x \in X$ beliebig waren, folgt: jeder Zustand aus D' ist völlig spezifiziert.

[24] Wir hatten vorausgesetzt, daß $\mathcal{A}$ in jedem Zustand für jeden Buchstaben aus X mindestens einen Übergang besitzt.

$2 \Rightarrow 3:$ Es gelte 2. Sei D' eine ergodische Menge von $C_{det}((x,q))$ so daß jeder Zustand in D' völlig spezifiziert ist. Sei $Y'' = \{(x,q)\},(x_1,R_1),(x_2,R_2),\ldots,(x_n,R_n)$ ein endlicher Lauf in $C_{det}((x,q))$ mit $(x_n,R_n) \in D'$. Dann ist $\gamma = x,x_1,\ldots,x_n$ ein endlicher Pfad in M, der die Bedingungen in 3 erfüllt. Dies folgt aus folgender Behauptung.
Behauptung : Sei $x,x_1,\ldots,x_n,y_{n+1},y_{n+2},\ldots$ ein Lauf in M. Dann gibt es für jedes $k \geq n$ einen endlichen Lauf

$$\{(x,q)\},(x_1,R_1),\ldots,(x_n,R_n),(y_{n+1},R_{n+1}),\ldots,(y_k,R_k)$$

in $C_{det}((x,q))$ mit $(y_i,R_i) \in D' \quad \forall i \geq n$.
Beweis der Behauptung : per Induktion über k

- Induktionsanfang : $k = n$
  Hier gibt es nichts zu zeigen.
- Induktionsschritt : $k \rightarrow k+1$
  Die Behauptung gelte für k. Sei

  $$\{(x,q)\},(x_1,R_1),\ldots,(x_n,R_n),(y_{n+1},R_{n+1}),\ldots,(y_k,R_k)$$

  ein entsprechender endlicher Lauf in $C_{det}((x,q))$. Es gilt also $(y_k,R_k) \in D'$. Da nun jeder Zustand von D' völlig spezifiziert ist, gilt dies insbesondere für (y_k,R_k). Dies bedeutet, daß es in $C_{det}((x,q))$ einen Übergang von (y_k,R_k) zu einem Zustand (y_{k+1},R_{k+1}) gibt, da (y_k,y_{k+1}) eine Transition in M ist.

Somit ist die Behauptung bewiesen. Dies impliziert nun, daß es für einen Lauf $Y = x,x_1,\ldots,x_n,y_{n+1},y_{n+2},\ldots$ von M einen in $\{(x,q)\}$ beginnenden, zu Y korrespondierenden Lauf

$$Y'' = \{(x,q)\},(x_1,R_1),\ldots,(x_n,R_n),(y_{n+1},R_{n+1}),\ldots$$

von $C_{det}((x,q))$ gibt. Aus der Potenzmengenkonstruktion folgt nun, daß es einen Lauf

$$Y' = (x,q),(x_1,q_1),\ldots,(x_n,q_n),(y_{n+1},q_{n+1}),\ldots$$

von $\mathcal{T}_{prob} \times \mathcal{A}$ gibt, mit $q_i \in R_i \ \forall i \in \mathbb{N}$. Das bedeutet aber, daß Y' zu Y korrespondiert und nur Zustände von C durchläuft.

$3 \Rightarrow 1:$ Es gelte 3 mit $\gamma = x,x_1,\ldots,x_n$ und (x,q). Wir wollen also zeigen, daß (x,q) periodisch ist. Z. z. ist also, daß der zugrundeliegende Graph von

$(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ eine ergodische Menge besitzt, die einen Zustand enthält, der (x,q) enthält. Dafür betrachten wir den eindeutigen endlichen Lauf

$$\{(x,q)\},(x_1,R_1),\ldots,(x_n,R_n) \quad \text{in } (\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q)).$$

Wir verlängern diesen, bis wir eine ergodische Menge D von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ erreichen. Es gelte also

$$\{(x,q)\},(x_1,R_1),\ldots,(x_n,R_n),(y_{n+1},R_{n+1}),\ldots,(y_{n+k},R_{n+k})$$

ist endlicher Lauf in $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ mit

$$(y_{n+k},R_{n+k}) \in D \ \wedge \ (y_{n+i},R_{n+i}) \notin E, \ \ i = 1,2\ldots(k-1),$$

wobei D eine ergodische Menge und E die Vereinigung aller ergodischen Mengen von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ ist. Nun gilt nach 3, daß es in $\mathcal{T}_{prob} \times \mathcal{A}$ einen in (x,q) beginnenden, endlichen, zu

$$x,x_1,\ldots,x_n,y_{n+1},\ldots,y_{n+k}$$

korrespondierenden Lauf gibt, der nur Zustände in C durchläuft. Dann folgt aber aufgrund der Potenzmengenkonstruktion, daß (y_{n+k},R_{n+k}) ein Element aus C enthält. Sei also

$$(y_{n+k},q_{n+k}) \in (y_{n+k},R_{n+k}) \text{ mit } (y_{n+k},q_{n+k}) \in C.$$

Da (x,q) und (y_{n+k},q_{n+k}) in der selben SCC von $\mathcal{T}_{prob} \times \mathcal{A}$ liegen, gibt es ein Eingabewort $\zeta \in X^*$, so daß der Automat $\mathcal{T}_{prob} \times \mathcal{A}$ vom Zustand (y_{n+k},q_{n+k}) bei Eingabe des Wortes ζ in den Zustand (x,q) übergeht. Sei nun z der Zustand des Automaten $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$ in den dieser vom Zustand (y_{n+k},R_{n+k}) durch Eingabe des Wortes ζ übergeht. Aus der Potenzmengenkonstruktion wird offensichtlich, daß $(x,q) \in z$ gilt. Ausserdem gehört z natürlich auch zu der ergodischen Menge D von $(\mathcal{T}_{prob} \times \mathcal{A})_{det}((x,q))$. Damit folgt 1.

$4 \Rightarrow 1:$ Dies ist trivialerweise erfüllt.

$1 \Rightarrow 4:$ Sei (x,q) periodisch. Dann wissen wir, daß Punkt 3 gilt. Sei $\gamma = x,x_1,\ldots,x_n$ ein endlicher Pfad in M, der die Bedingungen aus 3 erfüllt. Sei (x',q') ein weiterer Zustand aus C. Es ist also zu zeigen, daß (x',q') periodisch ist. Da

wir schon gezeigt haben, daß die Bedingungen aus Punkt 3 für (x',q') implizieren, daß (x',q') periodisch ist, zeigen wir also nun, daß Punkt 3 für (x',q') erfüllt ist. Da (x,q) und (x',q') in der SCC C von $\mathcal{T}_{prob} \times \mathcal{A}$ liegen, gibt es einen Pfad

$$(x',q'),(y_1,q_1),\ldots,(y_k,q_k),(x,q)$$

von (x',q') nach (x,q) im zugrundeliegenden Graphen von $\mathcal{T}_{prob} \times \mathcal{A}$ mit $(y_i,q_i) \in C,\ i = 1,2,\ldots,k$. Sei

$$\gamma' = x',y_1,\ldots,y_k,x,x_1,\ldots,x_n.$$

Dann erfüllen γ' und (x',q') Punkt 3. Sei nämlich Y ein Lauf in M, der γ' als Präfix hat. Dann gilt

$$Y = \beta\gamma\widetilde{Y},\ \text{ mit } \beta = x',y_1,\ldots,y_k.$$

Da (x,q) periodisch ist und aus der Wahl von γ folgt, daß es einen zu $\gamma\widetilde{Y}$ korrespondieren Lauf Y' von $\mathcal{T}_{prob} \times \mathcal{A}$ gibt, der in (x,q) beginnt und nur Zustände von C durchläuft. Dann ist aber

$$((x',q'),(y_1,q_1),\ldots,(y_k,q_k))Y'$$

ein zu Y korrespondierender Lauf von $\mathcal{T}_{prob} \times \mathcal{A}$, der in (x',q') beginnt und nur Zustände von C durchläuft. Somit ist Punkt 3 für (x',q') und γ' gezeigt.

□

Mit der Aussage dieses Lemmas können wir also Schritt 4 des Algorithmus relativ effizient bearbeiten.

Nun zu den einzelnen Schritten des Algorithmus: es sei angemerkt, daß wir die Größe eines Probabilistischen Programms mit $|\mathcal{T}_{prob}|$ bezeichnen und damit die Anzahl an Zuständen und Transitionen meinen. Ausserdem bezeichnen wir mit $|\mathcal{A}|$ die Größe eines NBAs und meinen damit die Anzahl an Zuständen und Übergängen.

Zu Schritt 1 : Wie schon in Satz 2.1, Seite 31 erwähnt, kann man in Zeit und Platz $O(|\varphi| \cdot 2^{|\varphi|})$ den NBA $\mathcal{A}'$ mit $\mathcal{L}_\omega(\mathcal{A}') = \mathcal{L}_\omega(\varphi)$ konstruieren.

Es sei jedoch angemerkt, daß man in diesem Schritt einige Optimierungen vornehmen kann, um die Größe des resultierenden NBAs relativ klein zu halten. Z. B. kann man auf Formelebene durch Umschreiben der gegebenen LTL-Formel bessere Resultate erzielen. Ausserdem gibt es einige Algorithmen, die mittels Bisumulations- bzw. Simulationsquotienten einen gegebenen NBA in einen kleineren NBA überführen, ohne die akzeptierte Sprache zu ändern. Wer mehr darüber

wissen will, siehe z. B. [SoBl00] und [EtHo00].
Zu Schritt 2 : Die notwendigen Veränderungen können so implentiert werden, daß der benötigte Zeitaufwand linear in $|\mathcal{T}_{prob}| + |\mathcal{A}|$ ist. Zusätzlich verändert sich die Größe von $\mathcal{T}_{prob}$ und $\mathcal{A}$ nicht wesentlich.
Zu Schritt 3 : Es ist klar daß $|\mathcal{T}_{prob} \times \mathcal{A}| = O(|\mathcal{T}_{prob}| \cdot |\mathcal{A}|)$. Ausserdem kann $\mathcal{T}_{prob} \times \mathcal{A}$ in Zeit $poly(O(|\mathcal{T}_{prob}| \cdot |\mathcal{A}|))$ konstruiert werden.
Zu Schritt 4 : Wir wollen also die periodischen Zustände (x,q) von $\mathcal{T}_{prob} \times \mathcal{A}$ bestimmen, mit $q \in F$. Mit Lemma 2.6, Seite 60 wissen wir, daß entweder alle Zustände einer SCC von $\mathcal{T}_{prob} \times \mathcal{A}$ periodisch sind, oder keiner.

Als erstes zerlegen wir also den zugrundeliegenden Graphen von $\mathcal{T}_{prob} \times \mathcal{A}$ in seine starken Zusammenhangskomponenten. Der Zeitaufwand für diese Zerlegung ist in $O(|\mathcal{T}_{prob} \times \mathcal{A}|)$ (siehe [JU94]). Sei $\mathbf{C} = \{C_1, \ldots, C_k\}$ die Menge dieser SCCs. Wir entfernen aus $\mathbf{C}$ nun alle SCCs von $\mathcal{T}_{prob} \times \mathcal{A}$, die keinen akzeptierenden Zustand enthalten. Sei also

$$\mathbf{C}' = \{C \in \mathbf{C} \mid \exists (x,q) \in C : q \in F\}.$$

Für alle $C \in \mathbf{C}'$ müssen wir nun überprüfen, ob ein beliebiger Zustand aus C periodisch ist, oder nicht. Dafür benutzen wir Bedingung 2 aus Lemma 2.6, Seite 60. Für jedes $C \in \mathbf{C}'$ wählen wir also ein beliebiges $(x_C, q_C) \in C$ und bilden $C_{det}((x_C, q_C))$. Nun berechnen wir die ergodischen Mengen des zugrundeliegenden Graphen von $C_{det}((x_C, q_C))$ (in Zeit linear zur Größe des Graphen) und überprüfen, ob für mindestens eine gilt, daß jeder in ihr enthaltene Zustand völlig spezifiziert ist, oder nicht. Falls dies der Fall ist, so sind nach Lemma 2.6 alle Zustände von C periodisch, ansonsten nicht.

Es ist natürlich nun von Interesse, den Wert

$$\sum_{C \in \mathbf{C}'} |C_{det}((x_C, q_C))|$$

abzuschätzen. Es gilt sicherlich

$$\sum_{C \in \mathbf{C}'} |C_{det}((x_C, q_C))| \;\leq\; \sum_{C \in \mathbf{C}} |C_{det}((x_C, q_C))|.$$

Sei $n_{\mathcal{A}}$ die Anzahl an Zuständen von $\mathcal{A}$ und $m_{\mathcal{T}}$ die Anzahl der Kanten im zugrundeliegenden Graphen von $\mathcal{T}_{prob}$. Wir werden jetzt zeigen, daß

$$\sum_{C \in \mathbf{C}} |C_{det}((x_C, q_C))| \;\leq\; 2 \cdot m_{\mathcal{T}} \cdot 2^{n_{\mathcal{A}}}$$

gilt.

Für $i \in \{1,2,\ldots,k\}$ sei A_i die Menge der Kanten im zugrundeliegenden Graphen von $(C_i)_{det}((x_{C_i}, q_{c_i}))$. Sei

$$\mathbf{A} \;=\; \cup_{i=1}^{k} A_i.$$

Wir definieren die Abbildung

$$g \;:\; \mathbf{A} \quad \longrightarrow \quad E_{\mathcal{T}} \times 2^{Q}$$

$$((x',R'),(x'',R'')) \quad \stackrel{g}{\longmapsto} \quad ((x',x''),R'),$$

wobei $E_{\mathcal{T}}$ die Menge der Kanten des zugrundeliegenden Graphen von $\mathcal{T}_{prob}$ ist und Q wie gewohnt die Menge der Zustände von $\mathcal{A}$ ist.

Wir zeigen jetzt, daß g injektiv ist, was $|\mathbf{A}| \leq m_{\mathcal{T}} \cdot 2^{n_{\mathcal{A}}}$ beweist. Nun sind aber alle $(C_i)_{det}((x_{C_i}, q_{C_i}))$ zusammenhängend, woraus die Behauptung folgt..

Zur Injektivität von g : Seien $((x',R'),(x'',R''))$ und $((\tilde{x}',\widetilde{R}'),(\tilde{x}'',\widetilde{R}''))$ aus $\mathbf{A}$ mit gleichem Bild unter g. Es gilt also :

$$\tilde{x}' = x' \;\wedge\; \tilde{x}'' = x'' \;\wedge\; \widetilde{R}' = R'.$$

Angenommen, $R'' \neq \widetilde{R}''$. Da die $(C_i)_{det}((x_{C_i}, q_{C_i}))$ deterministisch sind, folgt, daß $((x',R'),(x'',R''))$ und $((x',R'),(x'',\widetilde{R}''))$ zu unterschiedlichen $(C_i)_{det}((x_{C_i}, q_{C_i}))$ und $(C_j)_{det}((x_{C_j}, q_{C_j}))$ gehören. Nun berechnen wir aber für jedes $C_l \in \mathbf{C}$ jeweils nur ein $(C_l)_{det}((x_{C_l}, q_{C_l}))$. [25] Somit gilt auch $i \neq j$. Dann gilt aber

$$(x',R') \subset C_i \quad \wedge \quad (x',R') \subset C_j,$$

was ein Widerspruch ist, da C_i und C_j disjunkt sind.

Somit gilt also $R'' = \widetilde{R}''$ und die Injektivität von g ist gezeigt.

Der Zeitaufwand für Schritt 4 liegt also in $O(m_{\mathcal{T}} \cdot 2^{n_{\mathcal{A}}})$.

Zu Schritt 5 : Sei $n_{\mathcal{A}} = |Q|$ die Anzahl an Zuständen von $\mathcal{A}$. Sei $n_{\mathcal{T}}$ die Anzahl an Zuständen von $\mathcal{T}_{prob}$ und $m_{\mathcal{T}}$ die Anzahl an Transitionen in $\mathcal{T}_{prob}$. Dann gilt

$$|M'_{sdet}| \;=\; O((m_{\mathcal{T}} + n_{\mathcal{T}}) \cdot 2^{n_{\mathcal{A}}}).$$ [26]

[25] Bemerke, daß es für (x_{C_l}, q_{C_l}) viele verschiedene Möglichkeiten gibt.

[26] Bemerke, daß in M'_{sdet} nur solche Zustände vorkommen, die Mengen von Zuständen von $\mathcal{T}_{prob} \times \mathcal{A}$ sind, die dieselbe erste Komponente besitzen.

Zu Schritt 6 : Bestimme die ergodischen Mengen von M'_{sdet} mit klassischen Graphalgorithmen. Bestimme nun mit den Ergebnissen aus Schritt 4 die akzeptierenden ergodischen Mengen. Sei Q_1 die Vereinigung der akzeptierenden ergodischen Mengen, und sei Q_2 das Komplement von Q_1 in den Zuständen von M'_{sdet}. Seien alle Zustände von Q_1 mit einer neuen atomaren Aussage *akzept* markiert und alle Zustände von Q_2 seien nicht mit *akzept* markiert. Sei für einen Zustand q von $M_{sdet'}$ w_q die Wahrscheinlichkeit, daß ein in q beginnender Lauf von $M_{sdet'}$ die Formel $\neg akzept\, \mathcal{U} akzept$ erfüllt. Dann ist die Wahrscheinlichkeit, daß ein Lauf von $M_{sdet'}$ in einer akzeptierenden ergodischen Menge endet gleich

$$\sum_{q \in Q_1 \cup Q_2} p_0(q) \cdot w_q.$$

Zur Berechnung der w_q löst man ein Gleichungssystem in der Größe der Anzahl der Zustände von $M_{sdet'}$. Hierzu siehe Lemma 3.1, Seite 75, in Abschnitt 3.1.

Somit liegt der Zeitaufwand für Schritt 6 in $O(poly((m_{\mathcal{T}} + n_{\mathcal{T}}) \cdot 2^{n_{\mathcal{A}}}))$.

Zusammenfassend können wir also sagen, daß wir die Schritte 3 bis 6 mit einem Zeitaufwand in $O(poly(|\mathcal{T}_{prob}|) \cdot 2^{|\mathcal{A}|})$ durchführen können.

Es gilt also, daß wir den Wert

$$\mu(\mathbf{Y}_{\models \varphi})$$

mit einem Zeitaufwand berechnen können, der doppelt exponentiell in der Länge der Formel φ ist und polynomiell in der Größe des Systems $\mathcal{T}_{prob}$.

Kapitel 3

Probabilistisches *LTL*-Model Checking ohne *Buechi*-Automaten

Wie wir in Kapitel 2 gesehen haben, kann man die Tatsache, daß es zu jeder LTL-Formel φ einen *Buechi*-Automaten $\mathcal{A}$ mit $Words(\varphi) = \mathcal{L}_\omega(\mathcal{A})$ gibt, ausnutzen, um sowohl klassische Transitionssysteme als auch Probabilistische Programme auf ihre Erfüllbarkeit bezüglich der Formel φ zu testen. Wir wollen in diesem Kapitel ein Verfahren angeben, das für ein gegebenes Probabilistisches Programm $\mathcal{T}_{prob} = (M, AP, L)$ und eine LTL-Formel φ über AP ohne den Umweg über die *Buechi*-Automaten den Wert $\mu(\mathbf{Y}_{\models\varphi})$ berechnet. Dazu machen wir folgende Feststellung. Gegeben ein Probabilistisches Programm $\mathcal{T}_{prob} = (M, AP, L)$ und eine LTL-Formel φ über AP, die keine temporalen Operatoren enthält. φ ist also eine aussagenlogische Formel über AP. Das bedeutet, daß es nur vom ersten Zustand eines Laufes davon abhängt, ob dieser Lauf die Formel φ erfüllt. Z. B. erfüllt ein Lauf $Y = x_0, x_1, \ldots$ die Formel $\varphi_1 = a \wedge \neg(b \wedge c)$, mit a, b, c atomare Aussagen, genau dann, wenn $(a \in L(x_0) \wedge (b \in L(x_0) \rightarrow c \notin L(x_0)) \wedge (c \in L(x_0) \rightarrow b \notin L(x_0)))$, wenn also x_0 mit a markiert ist und nicht mit b und c markiert ist. Sei

$$X_{\varphi_1} = \{x \in X \mid a \in L(x) \ \wedge \ |L(x) \cap \{b, c\}| \leq 1\}.$$

Dann gilt

$$\mu(\mathbf{Y}_{\models\varphi_1}) = \sum_{x \in X_{\varphi_1}} p_0(x).$$

Es ist also einfach[1] möglich, für eine LTL-Formel φ ohne temporale Operatoren den Wert $\mu(\mathbf{Y}_{\models\varphi})$ zu berechnen. Der hier vorgestellte Algorithmus wird dies

[1] relativ zur Tatsache, daß das Erfüllbarkeitsproblem der Aussagenlogik *coNP*-vollständig ist

ausnutzen, indem er schrittweise temporale Operatoren aus einer gegebenen Formel eliminiert und durch neue atomare Aussagen ersetzt. Zugleich wird in jedem Schritt natürlich auch das Probabilistische Programm so angepaßt, daß die Wahrscheinlichkeit, die Formel zu erfüllen, erhalten bleibt. Es gibt also zwei Transformationen, eine für den "Until"-Operator und eine für den "Next Step"-Operator. Bevor wir nun auf diese eingehen werden, wollen wir noch die Erfülltrelation $\models$ für LTL-Formeln ohne temporale Operatoren auf Zustände erweitern.

Definition 3.0.14.
Gegeben eine LTL-Formel φ ohne temporale Operatoren über AP. Somit ist φ also eine aussagenlogische Formel über der Variablenmenge AP. Wir sagen nun, ein Zustand $x \in X$ erfüllt φ, i. Z. $x \models \varphi$, genau dann, wenn

$$\varphi\{^{a}/_{true},\ a \in L(x)\} \ = \ true,$$

wenn also die Belegung der atomaren Aussagen in $L(x)$ mit $true$ die Formel φ zu einer Tautologie machen. ■

Zusätzlich werden wir für dieses Kapitel noch die Definition von echten Läufen erweitern.

Definition 3.0.15. [**Echter in x beginnender Lauf**]
Sei $\mathcal{T}_{prob}$ ein Probabilistisches Programm und x_0 ein Zustand von $\mathcal{T}_{prob}$. Wir sagen

$$Y = x_0, x_1, x_2, \ldots$$

ist ein in x_0 beginnender echter Lauf von $\mathcal{T}_{prob}$, falls Y ein unendlicher Pfad im zugrundeliegenden Graphen von $\mathcal{T}_{prob}$ ist. Y unterscheidet sich also von einem echten Lauf von $\mathcal{T}_{prob}$ nur dadurch, daß keine Forderung an die initiale Wahrscheinlichkeit von x_0 gestellt wird. ■

3.1 Konstruktion für den "Until"-Operator

Gegeben ein Probabilistisches Programm $\mathcal{T}_{prob} = (M, AP, L)$ und eine LTL-Formel φ über AP. Sei $\phi \mathcal{U} \psi$ eine "temporal innerste" Teilformel von φ, d. h. ϕ und ψ enthalten jeweils keine temporalen Operatoren, bestehen also nur aus atomaren Aussagen und Booleschen Operatoren. Wir wollen nun diese Teilformel eliminieren. Das weitere Vorgehen sieht wie folgt aus. Wir werden ein neues Probabilistisches Programm $\mathcal{T}'_{prob}$ konstruieren, dessen Menge AP' der atomaren Aussagen aus AP

und einer neuen atomaren Aussage ρ besteht. Weiterhin sei φ' die Formel, die aus φ ensteht, indem man jedes Vorkommen von $\phi \mathcal{U} \psi$ durch ρ ersetzt. Es wird dann gelten:

$$\mu(\mathbf{Y}_{\models\varphi}) \;=\; \mu'(\mathbf{Y}'_{\models\varphi'}).^{2}$$

Zuerst werden wir die Zustände des Probabilistischen Programms in drei disjunkte Mengen $X^{\models}, X^{\not\models}, X^{?}$ aufteilen. $X^{\models}$ wird die Zustände x enthalten, für die ein in x beginnender Lauf mit Wahrscheinlichkeit 1 die Formel $\phi \mathcal{U} \psi$ erfüllt. Entsprechend wird $X^{\not\models}$ die Zustände x enthalten, für die ein in x beginnender Lauf die Formel $\phi \mathcal{U} \psi$ mit Wahrscheinlichkeit 0 erfüllt (es wird sogar gelten, daß für $x \in X^{\not\models}$ kein in x beginnender echter Lauf die Formel $\phi \mathcal{U} \psi$ erfüllt). In $X^{?}$ sind die Zustände x, für die ein in x beginnender Lauf die Formel $\phi \mathcal{U} \psi$ mit Wahrscheinlichkeit r, $0 < r < 1$ erfüllt. Dies geschieht in folgenden Schritten.

$X^{\models}$ und $X^{\not\models}$ seien die kleinsten Teilmengen von X, die die ersten drei der folgenden Eigenschaften erfüllen.

1. $X^{\models} \supset \{x \in X \mid x \models \psi\}$ und $X^{\not\models} \supset \{x \in X \mid x \models (\neg\phi \wedge \neg\psi\}$

Sei H der von den übrigen Zuständen $X \setminus (X^{\models} \cup X^{\not\models}) = \{x \in X \mid x \models (\phi \wedge \neg\psi)\}$ induzierte Teilgraph von (X,T). Sei H' die Menge aller Zustände in H, die im Graphen (X,T) einen direkten Nachfolger haben, der ψ erfüllt, also $H' = \{x \in H \mid \exists v \in X : (x,v) \in T \;\wedge\; v \models \psi\}$.

2. $X^{\not\models} \supset \{x \in H \mid H' \text{ ist von } x \text{ aus in } H \text{ nicht erreichbar}\}$.

Es wurden also noch solche Zustände x zu $X^{\not\models}$ hinzugefügt, für die jeder Pfad von x zu einem Zustand, der ψ erfüllt, durch einen Zustand führt, der $(\neg\phi \wedge \neg\psi)$ erfüllt. Somit gilt: keiner der in x beginnenden echte Läufe erfüllt die Formel $\phi \mathcal{U} \psi$. Bemerke, daß die Nachfolger eines in Schritt 2 zu $X^{\not\models}$ hinzugefügten Zustandes alle in $X^{\not\models}$ liegen.
Sei H'' die Menge aller Zustände in H, die im Graphen (X,T) einen direkten Nachfolger haben, der $(\neg\phi \wedge \neg\psi)$ erfüllt, also $H'' = \{x \in H \mid \exists v \in X : (x,v) \in T \;\wedge\; v \models (\neg\phi \wedge \neg\psi)\}$.

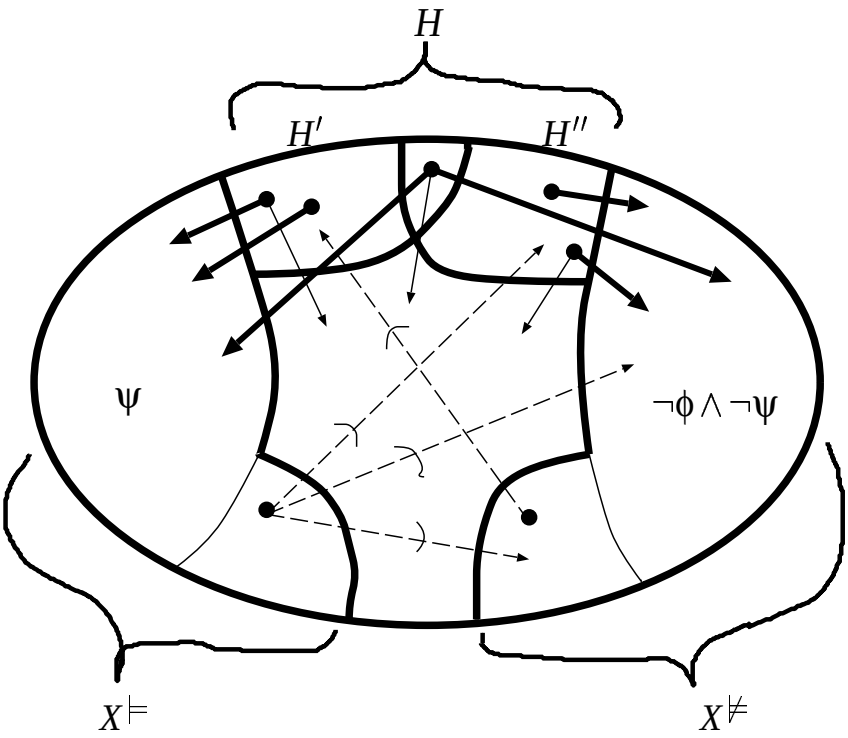
3. $X^{\models} \supset \{x \in H \mid (X^{\not\models} \cup H'') \text{ ist von } x \text{ aus in } H \text{ nicht erreichbar}\}$.

Es gilt nun für $x \in X^{\models}$, daß alle in x beginnenden echten Läufe $\phi \mathcal{U} \psi \;\vee\; \Box\phi$ erfüllen. Wir werden gleich zeigen, daß jedoch die Wahrscheinlichkeit, daß ein in x beginnender echter Lauf $\phi \mathcal{U} \psi$ nicht erfüllt, gleich 0 ist. Bemerke, daß die Nachfolger eines in Schritt 3 zu $X^{\models}$ hinzugefügten Zustandes alle in $X^{\models}$ liegen.

[2] Hier ist $\mathbf{Y}'_{\models\varphi'}$ die Menge der Läufe von $\mathcal{T}'_{prob}$, die die Formel φ' erfüllen.

4. $X^? = X \setminus (X^{\models} \cup X^{\not\models})$

Somit sind in $X^?$ alle anderen Zustände, die nicht $X^{\models}$ oder $X^{\not\models}$ zugeteilt wurden. Zur Veranschaulichung hier noch eine Graphik zur Partition von X.



Wir wollen jetzt die bereits gemachten Aussagen beweisen und zusätzlich einen Weg aufzeigen, wie man für $x \in X^?$ die Wahrscheinlichkeit berechnet, daß ein in x beginnender echter Lauf $\phi \mathcal{U} \psi$ erfüllt.

Lemma 3.1. *Für $x \in X$ sei q_x die Wahrscheinlichkeit, daß ein in x beginnender Lauf die Formel $(\phi \mathcal{U} \psi)$ erfüllt. Also*

$$q_x = \mu^x(\mathbf{Y}_{\models \phi \mathcal{U} \psi}) = \frac{\mu(\mathbf{Y}_{\models \phi \mathcal{U} \psi})}{p_0(x)}. \quad [3]$$

Dann erfüllen die q_x, $x \in X$, das folgende Gleichungssystem und stellen dessen eindeutige Lösung dar.

$$q_x = 1, \qquad x \in X^{\models}$$

[3] siehe Bemerkung 4 auf Seite 18

$$q_x = 0, \qquad x \in X^{\not\models}$$

$$q_x = \sum_{v \in X} p_{xv} \cdot q_v, \qquad x \in X^{?}$$

Beweis :

- $x \in X^{\not\models}$: Falls x in Schritt 1 zu $X^{\not\models}$ hinzugefügt wurde, so erfüllt x die Formel $\neg\phi \wedge \neg\psi$ und somit gilt für alle in x beginnenden echten Läufe, daß diese $\phi \mathcal{U} \psi$ nicht erfüllen. Falls x in Schritt 2 zu $X^{\not\models}$ hinzugefügt wurde, so gibt es für einen in x beginnenden echten Lauf zwei Möglichkeiten. Entweder er bleibt für immer in H, erfüllt somit $\phi \mathcal{U} \psi$ nicht. Oder er verlässt H und es gilt, daß der erste Zustand des Laufes, der nicht mehr in H ist, die Formel $\neg\phi \wedge \neg\psi$ erfüllt. Auch dann erfüllt der Lauf die Formel $\phi \mathcal{U} \psi$ nicht. Somit gilt, daß alle echten in x beginnenden Läufe die Formel $\phi \mathcal{U} \psi$ nicht erfüllen. Somit ist $\mathbf{Y}_{\models \phi \mathcal{U} \psi}$ eine messbare Teilmenge der nicht echten Läufe. Da die Menge der nicht echten Läufe Maß Null hat, folgt die Behauptung.

- $x \in X^{\models}$: Falls x in Schritt 1 zu $X^{\models}$ hinzugefügt wurde, so erfüllt x die Formel ψ und somit gilt für alle in x beginnenden echten Läufe, daß diese $\phi \mathcal{U} \psi$ erfüllen. Formal gilt also

  $$q_x = \mu^x(\mathbf{Y}_{\models \phi \mathcal{U} \psi}) = \mu^x(\{\text{alle in } x \text{ beginnenden Läufe}\}) = \mu^x(\Delta(x)) = 1.$$

  Sei nun x so, daß es in Schritt 3 zu $X^{\models}$ hinzugefügt wurde. Betrachten wir nun einen echten Lauf $Y = x, x_1, x_2, x_3, \ldots$. Mit der Wahrscheinlichkeit 1 erreicht dieser Lauf eine ergodische Menge C (verbleibt dann natürlich dort) und durchläuft jeden Zustand von C unendlich oft.[4] Es gibt nun zwei Möglichkeiten :

  - Y bleibt immer in H, also $x_i \in H \ \forall i \in \mathbb{N}$. Da Y jeden Zustand von C durchläuft, folgt $C \subset H$. Da aus C keine Kanten hinausführen (C ist ergodische Menge), wäre jeder Zustand von C dann in Schritt 2 zu $X^{\not\models}$ hizugefügt worden, also $C \subset X^{\not\models}$. Sei $j \in \mathbb{N}$ minimal, so daß $x_j \in C$. Dann ist $x, x_1, \ldots, x_j$ ein Weg von x nach $X^{\not\models}$ in H. Dies ist jedoch ein Widerspruch dazu, daß x in Schritt 3 zu $X^{\models}$ hizugefügt wurde.

[4] siehe Satz 1.2, Seite 24 ff.

– der vorige Fall tritt somit nicht ein und es gilt : Y verläßt H irgendwann. Sei $k \in \mathbb{N}$ minimal mit $x_k \notin H$. Da x in Schritt 3 zu $X^{\models}$ hinzugefügt wurde, gilt: x_k ist nicht in $X^{\not\models}$. Es folgt,

$$x_k \in X \setminus (H \cup X^{\not\models}) = \{x \in X \mid x \models \psi\}.$$

Da k minimal, gilt

$$x, x_1, \ldots, x_{k-1} \in H = \{x \in X \mid x \models (\phi \wedge \neg\psi)\}.$$

Also gilt $Y \models \phi \mathcal{U} \psi$, was die Behauptung zeigt.

Ganz formal sieht das so aus. Mit den Bezeichnungen von Satz 1.2 auf Seite 24, der Kantenmarkierung aus den nachfolgenden Bemerkungen (Seite 26), sowie dem obigen erhält man

$$Fair(x) \cap \Delta(x) \subset \mathbf{Y}_{\models \phi \mathcal{U} \psi}.$$

Es folgt

$$q_x = \mu^x(\mathbf{Y}_{\models \phi \mathcal{U} \psi}) \geq \mu^x(Fair(x) \cap \{\text{alle in } x \text{ beginnenden Läufe}\})$$

Da $\mu^x(Fair(x)) = 1$, folgt

$$q_x \geq \mu^x(Fair(x) \cap \Delta(x)) = \mu^x(\Delta(x)) = 1.$$

- $x \in X^?$: Bemerke, daß für jeden Lauf Y in M gilt:

$$Y \models \phi \mathcal{U} \psi \;\leftrightarrow\; Y \models \psi \vee (\phi \wedge X(\phi U \psi))$$

Sei nun $x \in X^?$. Dann gilt $x \models (\phi \wedge \neg\psi)$. Also folgt

$$\Delta(x) \cap \mathbf{Y}_{\models \phi \mathcal{U} \psi} = \Delta(x) \cap (\mathbf{Y}_{\models \psi} \cup (\mathbf{Y}_{\models \phi} \cap \mathbf{Y}_{\models X(\phi \mathcal{U} \psi)})) = \Delta(x) \cap \mathbf{Y}_{\models X(\phi \mathcal{U} \psi)}.$$

Man erhält weiterhin

$$\Delta(x) \cap \mathbf{Y}_{\models X(\phi \mathcal{U} \psi)} = x\mathbf{Y}_{\models \phi \mathcal{U} \psi} = \cup_{v \in X} x(\Delta(v) \cap \mathbf{Y}_{\models \phi \mathcal{U} \psi}),$$

wobei letzteres eine disjunkte Vereinigung ist. Somit gilt

$$q_x = \mu^x(\mathbf{Y}_{\models \phi \mathcal{U} \psi}) = \mu^x(\Delta(x) \cap \mathbf{Y}_{\models \phi \mathcal{U} \psi}) = \mu^x(\cup_{v \in X} x(\Delta(v) \cap \mathbf{Y}_{\models \phi \mathcal{U} \psi})) =$$

$$\sum_{v \in X} \mu^x(x(\Delta(v) \cap \mathbf{Y}_{\models \phi \mathcal{U} \psi})) = \sum_{v \in X} p_{xv} \cdot \mu^v(\mathbf{Y}_{\models \phi \mathcal{U} \psi}) = \sum_{v \in X} p_{xv} \cdot q_v.$$

Also stellen die q_x für das gegebene Gleichungssystem eine Lösung dar. Es bleibt noch zu zeigen, daß diese Lösung eindeutig ist. Dazu stellen wir zuerst fest, daß zwei Lösungen natürlich nur auf $X^?$ verschieden sein können. Seien also $\vec{a} = (a_x)_{x\in X}$ und $\vec{b} = (b_x)_{x\in X}$ zwei Lösungen des Gleichungssystems.[5] $\vec{a'} = (a_x)_{x\in X^?}$ und $\vec{b'} = (b_x)_{x\in X^?}$ seien die Einschränkung von $\vec{a}$, bzw. $\vec{b}$ auf $X^?$. $T = (p_{xy})_{x,y\in X}$ sei die Matrix der Transitionswahrscheinlichkeiten und $T' = (p_{xy})_{x,y\in X^?}$ deren Einschränkung auf $X^?$. Dann gilt

$$T(\vec{a}-\vec{b}) = \left\{ \begin{array}{rcl} 0 & : & x \notin X^? \\ a_x - b_x & : & x \in X^? \end{array} \right\}$$

Da für die Einschränkung von $(\vec{a}-\vec{b})$ auf $X^?$ auch gilt

$$(\vec{a}-\vec{b})' = \left\{ \begin{array}{rcl} 0 & : & x \notin X^? \\ a_x - b_x & : & x \in X^? \end{array} \right\}$$

folgt somit

$$T'(\vec{a'}-\vec{b'}) = \vec{a'}-\vec{b'}.$$

Es gilt also

$$\vec{a'}-\vec{b'} = T'(\vec{a'}-\vec{b'}) = (T')^2(\vec{a'}-\vec{b'}) = \ldots = (T')^k(\vec{a'}-\vec{b'})$$

für ein beliebiges $k \in \mathbb{N}$. Wir werden im folgenden zeigen, daß $\lim_{k\to\infty}(T')^k = \mathbf{0}$[6]. Daraus folgt dann, daß $\vec{a'}-\vec{b'} = 0$ und die Behauptung ist gezeigt.
Wir betrachten nun die Markov Kette $\widetilde{M} = (\widetilde{X},\ \widetilde{T},\ \tilde{p},\ \tilde{p_0})$ mit $\widetilde{X} = X \cup \{abs\}$, $\tilde{p_0}$ beliebig und

$$\widetilde{T} = (T \cap (X^? \times X^?)) \ \cup\ \{(x,abs) \mid x \in X^? \wedge \sum_{y\in X^?} p_{xy} < 1\} \ \cup\ \{(abs,abs)\}.$$

Weiterhin gelte

$$\tilde{p}_{uv} = \left\{ \begin{array}{rcl} p_{uv} & : & (u,v) \in T \\ 1 - \sum_{y\in X^?} p_{xy} & : & u \in X^? \wedge v = abs \\ 1 & : & (u,v) = (abs,abs) \end{array} \right\}$$

$\widetilde{M}$ besteht also aus dem Zustandsraum $X^?$ und einem zusätzlichen absorbierenden Zustand *abs*. Die Zustände in $X^?$ haben untereinander die gleichen Transitionen (mit den gleichen Transitionswahrscheinlichkeiten) wie in der ursprünglichen

[5] Es sei eine feste Anordnung der Elemente von X vorausgesetzt.
[6] **0** bezeichne die Nullmatrix

Markov Kette M. Deweiteren hat jeder Zustand aus $X^?$ eine Transition zu *abs* in $\widetilde{M}$, falls er in M Transitionen zu Zuständen außerhalb $X^?$ hatte. Die Transitionswahrscheinlichkeit ist in diesem Fall so gewählt, daß die Summe der ausgehenden Transitionswahrscheinlichkeiten eines Zustandes gerade 1 ergibt. Schließlich hat der Zustand *abs* noch eine Transition mit Wahrscheinlichkeit 1 zu sich selber. Unabhängig von der initialen Wahrscheinlichkeitsverteilung $\tilde{p_0}$ können wir folgende Beobachtung machen : $\{abs\}$ ist die einzige ergodische Menge in $\widetilde{M}$. Daß $\{abs\}$ eine ergodische Menge ist, ist offensichtlich. Angenommen es gäbe eine weitere ergodische Menge C in $\widetilde{M}$. Dann wäre $C \subset X^?$ und somit wäre C auch ergodische Menge in M.[7] Es folgt, daß die Zustände von C in Schritt 2 zu $X^{\not\models}$ hizugefügt worden wären, was ein Widerspruch ist.

Aus Abschnitt 1.3.2 wissen wir, daß jeder in einem beliebigen Zustand von $X^?$ beginnende Lauf von $\widetilde{M}$ mit Wahrscheinlichkeit 1 in *abs* enden wird. Bemerke, daß $((T')^k)_{xy}$ gleich der Wahrscheinlichkeit ist, daß ein in x beginnender Lauf nach k Schritten in y ist (dies läßt sich leicht unter Beachtung der Markov Eigenschaft per Induktion über k zeigen). Da nun ein in $x \in X^?$ beginnender Lauf mit Wahrscheinlichkeit 1 irgendwann *abs* erreicht (und dann dort verbleibt), können wir

$$\lim_{k\to\infty}((T')^k)_{xy} = 0 \qquad \forall (x,y) \in X^? \times X^?$$

folgern. Also gilt $\lim_{k\to\infty}(T')^k = \mathbf{0}$, was unser Argument vervollständigt. □

Für Teilformeln von φ der Art $\phi \mathcal{U} \psi$ mit ϕ und ψ Formeln ohne temporale Operatoren können wir also die Werte $q_x = \mu^x(\mathbf{Y}_{\models \phi \mathcal{U} \psi})$ durch Lösen eines Gleichungssystems berechnen. Mit Hilfe dieser Werte können wir die bereits erwähnte Konstruktion durchführen.

Die Konstruktion

Wir definieren ein neues Probabilistisches Programm $\mathcal{T}'_{prob} = (M', AP', L')$, wobei $AP' = AP \cup \rho$ mit $\rho \notin AP$. ρ wird für die Teiformel $\phi \mathcal{U} \psi$ stehen. Die Zustände von M' sind von der Form (x,ρ), falls $x \in X^{\models}$, $(x,\neg\rho)$, falls $x \in X^{\not\models}$ und $(x,\rho),(x,\neg\rho)$, falls $x \in X^?$. Ein Zustand (x,ρ) erfüllt dieselben atomaren Aussagen wie x und zusätzlich auch noch ρ. Ein Zustand $(x,\neg\rho)$ erfüllt nur dieselben atomaren Aussagen wie x. Die Transitionen und deren Wahrscheinlichkeiten werden so definiert, daß

[7] Beachte, daß Transitionen, die in M aus $X^?$ hinausführen, in $\widetilde{M}$ durch Transitionen nach *abs* simuliert werden.

wir folgende Bedeutung erhalten. Die Wahrscheinlichkeitsmasse der in (x,ρ) beginnenden Läufe ist gleich der Wahrscheinlichkeitsmasse der in x beginnenden und $\phi \mathcal{U} \psi$ erfüllenden Läufe. Genauer impliziert jede Transition (x,y) aus M ein oder zwei Transitionen in M'. Wir definieren die Transitionswahrscheinlichkeit für eine Transition $((x,\rho_1),(y,\rho_2)) \in T', \quad \rho_1,\rho_2 \in \{\rho,\neg\rho\}$ als die Wahrscheinlichkeit, daß für einen in x beginnender Lauf $Y = x,x_1,x_2,\ldots$ von M gilt, daß $x_1 = y$ und $x_1,x_2,\ldots$ erfüllt ρ_2 unter der Voraussetzung, daß Y ρ_1 erfüllt (wobei hier ρ für $\phi \mathcal{U} \psi$ und $\neg\rho$ für $\neg(\phi \mathcal{U} \psi)$ stehen). Nun zum formalen Teil:

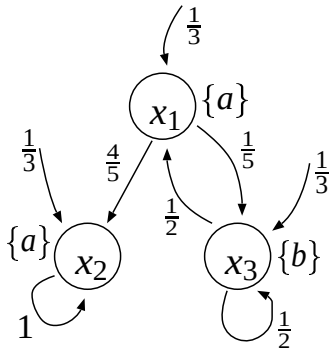
Definition 3.1.1. Sei $\mathcal{T}'_{prob} = (M', AP', L')$ mit $M' = (X', T', p', p'_0)$ folgendes Probabilistische Programm. Für $x \in X$ sei q_x wie in Lemma 3.1, Seite 75.

- $AP' = AP \cup \{\rho\}, \ \rho \notin AP$
- $X' = \{(x,\rho) \mid x \in X^{\models} \cup X^{?}\} \quad \cup \quad \{(x,\neg\rho) \mid x \in X^{\not\models} \cup X^{?}\}$
- $L'(x,\rho) = L(x) \cup \{\rho\}$
  $L'(x,\neg\rho) = L(x)$
- $p'_0((x,\rho)) = p_0(x) q_x \quad \wedge \quad p'_0((x,\neg\rho)) = p_0(x)(1-q_x)$
- Im folgenden gelte $\rho_1,\rho_2 \in \{\rho,\neg\rho\}$. Sei T' die kleinste Teilmenge von T, die folgende Eigenschaften erfüllt: für alle $(x,y) \in T$ gilt
  - $x,y \in X^{\models} \cup X^{\not\models} \implies ((x,\rho_1),(y,\rho_2)) \in T'$
    Bemerke, daß nur eine Transition in T' eingefügt wird.
    Wir definieren $p'_{(x,\rho_1)(y,\rho_2)} = p_{xy}$.
  - $x \in X^{\models} \cup X^{\not\models} \ \wedge \ y \in X^{?} \implies ((x,\rho_1),(y,\rho))$ und $((x,\rho_1),(y,\neg\rho)) \in T'$
    Bemerke, daß ρ_1 eindeutig durch x bestimmt ist.
    Wir definieren $\begin{aligned} p'_{(x,\rho_1)(y,\rho)} &= p_{xy} q_y \\ p'_{(x,\rho_1)(y,\neg\rho)} &= p_{xy}(1-q_y). \end{aligned}$
  - $x \in X^{?} \ \wedge \ y \in X^{\models} \implies ((x,\rho),(y,\rho)) \in T'$
    Wir definieren $p'_{(x,\rho)(y,\rho)} = \frac{p_{xy}}{q_x}$.
  - $x \in X^{?} \ \wedge \ y \in X^{\not\models} \implies ((x,\neg\rho),(y,\rho)) \in T'$
    Wir definieren $p'_{(x,\neg\rho)(y,\neg\rho)} = \frac{p_{xy}}{1-q_x}$.
  - $x,y \in X^{?} \implies ((x,\rho),(y,\rho))$ und $((x,\neg\rho),(y,\neg\rho)) \in T'$
    Wir definieren $\begin{aligned} p'_{(x,\rho)(y,\rho)} &= p_{xy} \frac{q_y}{q_x} \\ p'_{(x,\neg\rho)(y,\neg\rho)} &= p_{xy} \frac{(1-q_y)}{1-q_x}. \end{aligned}$

■

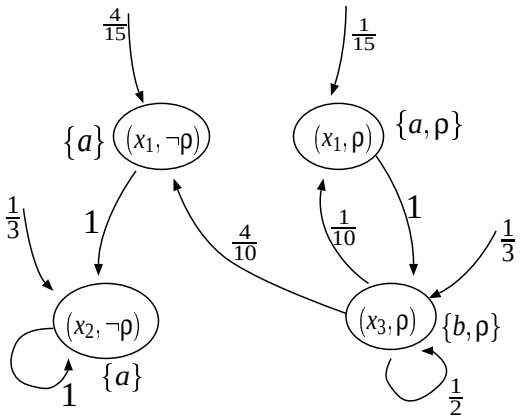
Bevor wir fortfahren soll nun ein kleines Beispiel die obige Konstruktion veranschaulichen.

Beispiel 3.1.1. Gegeben ist ein Probabilistisches Programm mit den drei Zuständen x_1, x_2 und x_3. Die Aussagenmenge ist $AP = \{a, b\}$, und wir betrachten die Formel $a \mathcal{U} b$. Die Transitionen und deren Wahrscheinlichkeiten, sowie die initialen Wahrscheinlichkeiten sind durch folgende Graphik dargestellt.



$$X^{\models} = \{x_3\}$$
$$X^{\not\models} = \{x_2\}$$
$$X^{?} = \{x_1\}$$
$$q_{x_3} = 1$$
$$q_{x_2} = 0$$
$$q_{x_1} = \tfrac{1}{5}$$

Durch die obige Konstruktion erhalten wir



Sei nun φ' diejenige Formel über AP', die aus φ entsteht, indem man jedes Vorkommen von $\phi \mathcal{U} \psi$ durch ρ ersetzt. Wie schon erwähnt werden wir zeigen, daß

$$\mu(\mathbf{Y}_{\models\varphi}) \;=\; \mu'(\mathbf{Y}'_{\models\varphi'}), \quad \text{wobei } \mu' \text{ das Maß des Folgenraums von } \mathcal{T}'_{prob} \text{ ist.}$$

Dazu zeigen wir erst zwei Lemmata, aus denen dann die Behauptung ganz einfach folgt.

Definition 3.1.2. [Die Projektion π]
Für $Y' = (x_0,\rho_0),(x_1,\rho_1),(x_2,\rho_2),\ldots$ Lauf in M' $(\rho_0,\rho_1,\rho_2,\ldots \in \{\rho,\neg\rho\})$ heißt $\pi(Y') = x_0,x_1,x_2,\ldots$ die Projektion von Y', also

$$\pi \ : \ (X')^\omega \longrightarrow X^\omega.$$

Bemerke, daß wir π auch auf endliche Pfade von M' anwenden werden. Wir meinen dann die offensichtliche Abbildung $\pi : \cup_{k\in\mathbb{N}}(X')^k \to \cup_{k\in\mathbb{N}}X^k$. ■

Wir zeigen jetzt, daß für eine messbare Teilmenge $A \subset X^\omega$ gilt :

$$\mu(A) = \mu'(\pi^{-1}(A)).$$

Es genügt jedoch, dies für alle Basiszylinder von M zu zeigen.[8]

Lemma 3.2. *Für alle $x_0,x_1,\ldots,x_n \in X, n \in \mathbb{N}$ gilt*

$$\mu(\Delta(x_0,x_1,\ldots,x_n)) = \mu'(\pi^{-1}(\Delta(x_0,x_1,\ldots,x_n))).$$

Beweis : Seien $x_0,x_1,\ldots,x_n \in X$ und $\rho_0,\rho_1,\ldots,\rho_n,\tilde\rho,\tilde{\tilde\rho}$ aus $\{\rho,\neg\rho\}$. Zuerst wollen wir die Menge $\pi^{-1}(\Delta(x_0,x_1,\ldots,x_n))$ bestimmen. Dazu bemerken wir folgendes. Sei $(y,\tilde\rho)$ ein Zustand in X' und $(x,y) \in T$ eine Transition in M. Dann gibt es genau eine Transition $((x,\tilde{\tilde\rho})(y,\tilde\rho))$ in M', denn entweder gilt

- $x \in X^{\models} \cup X^{\not\models}$. Dann gibt es nur einen Zustand in M' mit erster Komponente gleich x. Oder es gilt
- $x \in X^?$. Dann gilt $\tilde{\tilde\rho} = \tilde\rho$, d. h. beide Zustände müssen in ihrer zweiten Komponente übereinstimmen (siehe Definition 3.1.1 von $\mathcal{T}'_{prob}$).

Das heißt, daß es für $x'_n = (x_n,\tilde\rho)$ genau einen Pfad $x'_0,x'_1,\ldots,x'_n$ in M' gibt mit $\pi(x'_0,x'_1,\ldots,x'_n) = x_0,x_1,\ldots,x_n$. Es kann also in M' höchstens zwei Pfade geben, deren Projektion gleich $x_0,x_1,\ldots,x_n$ ist. Falls $(x_n,\rho) \in X'$, so sei γ^ρ der eindeutige in (x_n,ρ) endende Pfad, dessen Projektion gleich $x_0,x_1,\ldots,x_n$ ist. Falls $(x_n,\neg\rho) \in X'$, so sei $\gamma^{\neg\rho}$ der eindeutige in $(x_n,\neg\rho)$ endende Pfad, dessen Projektion gleich $x_0,x_1,\ldots,x_n$ ist. Dann gilt also

$$\pi^{-1}(\Delta(x_0,x_1,\ldots,x_n)) = \bigcup_{(x_n,\rho)\in X'} \Delta'(\gamma^\rho) \ \cup \ \bigcup_{(x_n,\neg\rho)\in X'} \Delta'(\gamma^{\neg\rho})$$

[8] für detaillierte Erklärung siehe [Bau78]

Somit ist $\pi^{-1}(\Delta(x_0,x_1,\ldots,x_n))$ meßbar im Folgenraum von M' und es gilt

$$\mu'(\pi^{-1}(\Delta(x_0,x_1,\ldots,x_n))) = \sum_{(x_n,\rho)\in X'} \mu'(\Delta'(\gamma^\rho)) \; + \sum_{(x_n,\neg\rho)\in X'} \mu'(\Delta'(\gamma^{\neg\rho}))$$

Wir zeigen jetzt

$$\mu'(\Delta'(\gamma^\rho)) = \mu(\Delta(x_0,x_1,\ldots,x_n)) \times q_{x_n} \tag{3.1}$$

und

$$\mu'(\Delta'(\gamma^{\neg\rho})) = \mu(\Delta(x_0,x_1,\ldots,x_n)) \times (1-q_{x_n}), \tag{3.2}$$

womit die Behauptung folgt.[9]
Wir zeigen 3.1 und 3.2 nun per Induktion über n.

- Induktionsanfang : $n = 0$.
  Für $x_0 \in X$ gilt : falls $(x_0,\rho) \in X'$, so ist $\gamma^\rho = (x_0,\rho)$ und

  $$\mu'(\Delta'(\gamma^\rho)) = p'_0((x_0,\rho)) = p_0(x_0)q_{x_0} = \mu(\Delta(x_0)) \times q_{x_0}.$$

  Falls $(x_0,\neg\rho) \in X'$, so ist $\gamma^{\neg\rho} = (x_0,\neg\rho)$ und

  $$\mu'(\Delta'(\gamma^{\neg\rho})) = p'_0((x_0,\neg\rho)) = p_0(x_0)(1-q_{x_0}) = \mu(\Delta(x_0)) \times (1-q_{x_0}).$$

- Induktionsschritt : sei die Behauptung für Basiszylinder der Länge $\leq n$ bewiesen. Seien $x_0,x_1,\ldots,x_n,x_{n+1} \in X$. Sei

  $$u'_0,u'_1,\ldots,u'_n,(x_{n+1},\rho) = \gamma^\rho \quad \text{und} \quad v'_0,v'_1,\ldots,v'_n,(x_{n+1},\neg\rho) = \gamma^{\neg\rho}$$

  Es gilt nun
  $\mu'(\Delta'(\gamma^\rho)) =$
  $\mu'(\Delta'(u'_0,u'_1,\ldots,u'_n,(x_{n+1},\rho))) = \mu'(\Delta'(u'_0,u'_1,\ldots,u'_n)) \times p'_{u'_n(x_{n+1},\rho)}.$

  - $u'_n \models \rho$: $\ldots = (\mu(\Delta(x_0,x_1,\ldots,x_n)) \times q_n) \times p_{x_nx_{n+1}} \frac{q_{n+1}}{q_n}$
    $= \mu(\Delta(x_0,x_1,\ldots,x_n,x_{n+1})) \times q_{n+1}$.[10]
  - $u'_n \not\models \rho$: $\ldots = (\mu(\Delta(x_0,x_1,\ldots,x_n)) \times (1-q_n)) \times p_{x_nx_{n+1}} \frac{1-q_{n+1}}{1-q_n}$
    $= \mu(\Delta(x_0,x_1,\ldots,x_n,x_{n+1})) \times (1-q_{n+1})$.

[9] Bemerke, daß falls es nur (x_n,ρ) in X' gibt, so ist $q_{x_n} = 1$ und falls es nur $(x_n,\neg\rho)$ in X' gibt, so ist $(1-q_{x_n}) = 1$.

[10] Bemerke, daß falls $x,y \in X^{\models}$, dann ist $p'_{(x,\rho)(y,\rho)} = p_{xy} = p_{xy}\frac{1}{1} = p_{xy}\frac{q_y}{q_x}$ und entsprechend die restlichen Fälle.

Weiterhin gilt
$\mu'(\Delta'(\gamma^{\neg\rho})) =$
$\mu'(\Delta'(v'_0, v'_1, \ldots, v'_n, (x_{n+1}, \neg\rho))) = \mu'(\Delta'(v'_0, v'_1, \ldots, v'_n)) \times p'_{v'_n(x_{n+1}, \neg\rho)}$.

- $u'_n \models \rho$: $\ldots = (\mu(\Delta(x_0, x_1, \ldots, x_n)) \times q_n) \times p_{x_n x_{n+1}} \frac{q_{n+1}}{q_n}$
  $= \mu(\Delta(x_0, x_1, \ldots, x_n, x_{n+1})) \times q_{n+1}$.
- $u'_n \not\models \rho$: $\ldots = (\mu(\Delta(x_0, x_1, \ldots, x_n)) \times (1 - q_n)) \times p_{x_n x_{n+1}} \frac{1-q_{n+1}}{1-q_n}$
  $= \mu(\Delta(x_0, x_1, \ldots, x_n, x_{n+1})) \times (1 - q_{n+1})$.

Somit folgen die Gleichungen 3.1 und 3.2 und der Beweis des Lemmas ist fertig. □

Mit der Aussage des Lemmas folgt nun insbesondere: für jede LTL-Formel $\tilde{\varphi}$ über AP gilt

$$\mu(\mathbf{Y}_{\models\tilde{\varphi}}) = \mu'(\mathbf{Y}'_{\models\tilde{\varphi}}).$$

Dies liegt daran, daß

$$\pi^{-1}(\mathbf{Y}_{\models\tilde{\varphi}}) = \mathbf{Y}'_{\models\tilde{\varphi}}.$$

Somit haben die Probabilistischen Systeme $\mathcal{T}_{prob}$ und $\mathcal{T}'_{prob}$ die gleiche Wahrscheinlichkeitsverteilung für LTL-Formeln über AP. Es gilt also auch

$$\mu(\mathbf{Y}_{\models\varphi}) = \mu'(\mathbf{Y}'_{\models\varphi}) \tag{3.3}$$

für die Formel φ aus unserer Konstruktion. Um die gewünschte Eigenschaft unserer Konstruktion nachzuweisen, müssen wir also noch zeigen, daß

$$\mu'(\mathbf{Y}'_{\models\varphi}) = \mu'(\mathbf{Y}'_{\models\varphi'}) \quad [11]$$

gilt. Dies ist aber gewährleistet, wenn gilt

$$\mu'(\mathbf{Y}'_{\models X^k(\phi\,\mathcal{U}\psi)}) = \mu'(\mathbf{Y}'_{\models X^k\rho}) \qquad \forall k \in \mathbb{N},$$

wenn also für alle $k \in \mathbb{N}$ und einen Lauf $Y' = x'_0, x'_1, x'_2, \ldots$ mit Wahrscheinlichkeit 1 gilt: $x'_k \models \rho$ gdw $x'_k, x'_{k+1}, \ldots \models \phi\,\mathcal{U}\psi$. Aufgrund der Tatsache, daß

$$\mathbf{Y}'_{\models X^k\tilde{\varphi}} = \bigcup_{x'_0, \ldots x'_{k-1} \in X'} \Delta'(x'_0, \ldots x'_{k-1})\mathbf{Y}'_{\models\tilde{\varphi}}$$

muss diese Eigenschaft nur für $k = 0$ gezeigt werden. Genau dies leistet das folgende Lemma.

[11] φ' bezeichnete die Formel über AP' die aus φ entsteht, indem man alle Vorkommen von $\phi\,\mathcal{U}\psi$ durch ρ ersetzt.

Lemma 3.3.

$$\mu'(\mathbf{Y}'_{\models(\phi\,\mathcal{U}\psi)}) = \mu'(\mathbf{Y}'_{\models\rho})$$

Beweis : Es gelten folgende disjunkte Vereinigungen:

$$\mathbf{Y}'_{\models\rho} \;=\; (\mathbf{Y}'_{\models\phi\,\mathcal{U}\psi} \cap \mathbf{Y}'_{\models\rho}) \;\cup\; (\mathbf{Y}'_{\models\neg(\phi\,\mathcal{U}\psi)} \cap \mathbf{Y}'_{\models\rho}) \tag{3.4}$$

und

$$\mathbf{Y}'_{\models\phi\,\mathcal{U}\psi} \;=\; (\mathbf{Y}'_{\models\phi\,\mathcal{U}\psi} \cap \mathbf{Y}'_{\models\rho}) \;\cup\; (\mathbf{Y}'_{\models\phi\,\mathcal{U}\psi} \cap \mathbf{Y}'_{\models\neg\rho}). \tag{3.5}$$

Falls also

$$\mu'(\mathbf{Y}'_{\models\neg(\phi\,\mathcal{U}\psi)} \cap \mathbf{Y}'_{\models\rho}) = 0 \;\text{ und }\; \mu'(\mathbf{Y}'_{\models\phi\,\mathcal{U}\psi} \cap \mathbf{Y}'_{\models\neg\rho}) = 0,$$

so folgt mit 3.4 und 3.5 die Behauptung. Sei $Fair'$ die Menge aller Läufe in M', die in einer ergodischen Menge von M' enden und jeden Zustand von dieser Menge unendlich oft besuchen. Wir wissen von Abschnitt 1.3.2 auf Seite 21, daß $\mu'(Fair')$ gleich 1 ist, daß also das Komplement $\neg Fair$ eine Nullmenge ist.

- $\mu'(\mathbf{Y}'_{\models\neg(\phi\,\mathcal{U}\psi)} \cap \mathbf{Y}'_{\models\rho}) = 0$: wir zeigen

  $$\mathbf{Y}'_{\models\neg(\phi\,\mathcal{U}\psi)} \cap \mathbf{Y}'_{\models\rho} \;\subset\; \neg Fair \cap \mathbf{Y}'_{\models\rho},$$

  woraus die Behauptung folgt. Sei also $Y' = x'_0, x'_1, \ldots \in \mathbf{Y}'_{\models\neg(\phi\,\mathcal{U}\psi)} \cap \mathbf{Y}'_{\models\rho}$, somit gilt $x'_0 \models \rho$, also $x'_0 = (x_0, \rho)$. Es gibt nun zwei Möglichkeiten:

  - $x_0 \in X^{\models}$: sei $M'_{X^{\models}}$ der Teilgraph von M', der von den Zuständen von M' induziert wird, deren erste Komponente in $X^{\models}$ liegt. Dann ist $M'_{X^{\models}}$ isomorph zu dem von $X^{\models}$ induzierten Teilgraphen von M (siehe Konstruktion von M' (Definition 3.1.1, Seite 80)). Wir wissen ja, daß Y' $\neg(\phi\,\mathcal{U}\psi)$ erfüllt und wollen zeigen, daß $Y' \notin Fair$ gilt. Bemerke dazu folgendes: alle Zustände von $M'_{X^{\models}}$ erfüllen entweder $(\phi \wedge \neg\psi)$ oder ψ, da die erste Komponente dieser Zustände in $X^{\models}$ liegt. Ausserdem gilt für alle Transitionen (x', y') in M', die aus $M'_{X^{\models}}$ herausführen, daß x' die Formel ψ erfüllt.[12] Somit gilt: jeder in x'_0 beginnende Lauf von M', der $M'_{X^{\models}}$ verlässt, erfüllt die Formel $\phi\,\mathcal{U}\psi$. Daraus folgt, daß Y' den Teilgraphen $M'_{X^{\models}}$ nie verlässt. Nun gilt aber für jede ergodische Menge in $M'_{X^{\models}}$, daß diese auch Zustände enthält, die ψ erfüllen.$^{(*)}$ Würde

[12] siehe Schritt 3 zur Partitionierung von X auf Seite 74

$Y' \in Fair$ gelten, so würde Y' in einer solchen ergodischen Menge enden und jeden ihrer Zustände unendlich oft durchlaufen. Somit würde $Y' \models \phi \mathcal{U} \psi$ gelten, was ein Widerspruch ist. Also folgt $Y' \notin Fair$.
Zu $^{(*)}$: Sei C' eine ergodische Menge von $M'_{X^{\models}}$ und C die Projektion von C' auf die erste Komponente derer Zustände. Dann ist C auch ergodische Menge von dem von $X^{\models}$ induzierten Teilgraphen von M. Angenommen C enthält keinen Zustand, der ψ erfüllt. Dann sind also alle Zustände von C in Schritt 3 auf Seite 74 $X^{\models}$ zugeteilt worden. Somit gibt es keine Nachfolger von C, die nicht in $X^{\models}$ liegen. Dann ist C aber ergodische Menge von M, was ein Widerspruch zu $C \subset X^{\models}$ ist.

– $x_0 \in X^?$: betrachte den von der Zustandsmenge $X^?_\rho = \{(x,\rho) \mid x \in X^?\}$ induzierten Teilgraphen $M'_{X^?_\rho}$ von M'. Dann ist $M'_{X^?_\rho}$ isomorph zu dem von $X^?$ induzierten Teilgraphen $M_{X^?}$ von M und es gilt: alle Transitionen, die aus $M'_{X^?_\rho}$ hinausführen, führen zu einem Zustand von $M'_{X^{\models}}$ (siehe Konstruktion von M'). Ausserdem enthält $M'_{X^?_\rho}$ keine ergodische Menge von M'.$^{(**)}$ Falls also Y' die Menge $X^?_\rho$ nicht verlässt, so kann Y' zwar in eine ergodische Menge von M' hineinlaufen, aber auf keinen Fall alle Zustände dieser Menge unendlich oft durchlaufen. Somit gilt $Y' \notin Fair$.
Falls aber Y' die Menge $X^?_\rho$ verlässt, so sei x'_i der erste Zustand von Y', der nicht in $X^?_\rho$ enthalten ist. Wir wissen, daß gilt:

  * $x'_j \models (\phi \wedge \neg\psi), \quad j = 0,1,\ldots,(i-1)$
  * $x_i \in M'_{X^{\models}}$

  Da $Y' \not\models (\phi \mathcal{U} \psi)$, folgt $x_i,', x'_{i+1}, \ldots \not\models (\phi \mathcal{U} \psi)$. Dann wissen wir aber aus dem schon behandelten Teil, daß $x_i,', x'_{i+1}, \ldots \notin Fair$. Daraus folgt nun $Y' \notin Fair$.
  Zu $^{(**)}$: Angenommen C' ist ergodische Menge von M' und $C' \subset X^?_\rho$. Dann ist C' auch ergodische Menge von $M'_{X^?_\rho}$. Sei C die Projektion der Zustände von C auf deren erste Komponente. Dann ist $C \subset X^?$ und C ist ergodische Menge von $M_{X^?}$. Somit gibt es keine Transitionen von C nach $X^?$. Es gibt aber auch keine Transitionen von C nach $X^{\models}$, da es sonst eine entsprechende Transition in M' gäbe und C' somit keine ergodische Menge von M' wäre. Das ist aber ein Widerspruch, da nämlich dann die Zustände von C zu $X^{\not\models}$ hinzugefügt worden wären.

- $\mu'(\mathbf{Y}'_{\models \phi \mathcal{U} \psi} \cap \mathbf{Y}'_{\models \neg \rho}) = 0$: wir zeigen

$$\mathbf{Y}'_{\models \phi \mathcal{U} \psi} \cap \mathbf{Y}'_{\models \neg \rho} \subset \neg Fair \cap \mathbf{Y}'_{\models \neg \rho},$$

woraus die Behauptung folgt. Sei also $Y' = x'_0, x'_1, \ldots \in \mathbf{Y}'_{\models \phi \mathcal{U} \psi} \cap \mathbf{Y}'_{\models \neg \rho}$, somit gilt $x'_0 \models \neg \rho$, also $x'_0 = (x_0, \neg \rho)$. Es gilt nun : $x_0 \in X^?$.

  - Sei $M'_{X^{\not\models}}$ der Teilgraph von M', der von den Zuständen von M' induziert wird, deren erste Komponente in $X^{\not\models}$ liegt. Dann ist $M'_{X^{\not\models}}$ isomorph zu dem von $X^{\not\models}$ induzierten Teilgraphen von M (siehe Konstruktion von M' (Definition 3.1.1, Seite 80)). Bemerke folgendes: alle Zustände von $M'_{X^{\not\models}}$ erfüllen entweder $(\phi \wedge \neg \psi)$ oder $(\neg \phi \wedge \neg \psi)$, da die erste Komponente dieser Zustände in $X^{\not\models}$ liegt. Ausserdem gilt für alle Transitionen (x', y') in M', die aus $M'_{X^{\not\models}}$ herausführen, daß x' die Formel $\neg \phi \wedge \neg \psi$ erfüllt, da alle Nachfolger eines Zustandes der in Schritt 2 auf Seite 74 zu $X^{\not\models}$ hinzugefügt wurde, wiederum in $X^{\not\models}$ liegen. Somit gilt für alle in einem Zustand $(x, \neg \rho), x \in X^{\not\models}$ beginnenden Läufe, daß diese die Formel $\phi \mathcal{U} \psi$ nicht erfüllen. Daraus folgt, $x_0 \notin X^{\not\models}$, also $x_0 \in X^?$.
  - $x_0 \in X^?$: betrachte den von der Zustandsmenge $X^?_{\neg \rho} = \{(x, \neg \rho) \mid x \in X^?\}$ induzierten Teilgraphen $M'_{X^?_{\neg \rho}}$ von M'. Dann ist $M'_{X^?_{\neg \rho}}$ isomorph zu dem von $X^?$ induzierten Teilgraphen $M_{X^?}$ von M und es gilt: alle Transitionen, die aus $M'_{X^?_{\neg \rho}}$ hinausführen, führen zu einem Zustand von $M'_{X^{\not\models}}$ (siehe Konstruktion von M'). Daraus folgt, daß Y' die Menge $X^?_{\neg \rho}$ nie verlässt, da Y' sonst aufgrund des oben gezeigten $\phi \mathcal{U} \psi$ nicht erfüllen würde. Nun gilt auch hier, daß $M'_{X^?_{\neg \rho}}$ keine ergodische Menge von M' enthält.$^{(***)}$ Also kann Y' zwar in eine ergodische Menge von M' hineinlaufen, aber auf keinen Fall alle Zustande dieser Menge unendlich oft durchlaufen. Somit gilt $Y' \notin Fair$.
    Zu $^{(***)}$: Angenommen C' ist ergodische Menge von M' und $C' \subset X^?_{\neg \rho}$. Dann ist C' auch ergodische Menge von $M'_{X^?_{\neg \rho}}$. Sei C die Projektion der Zustände von C auf deren erste Komponente. Dann ist $C \subset X^?$ und C ist ergodische Menge von $M_{X^?}$. Somit gibt es keine Transitionen von C nach $X^?$. Es gibt aber auch keine Transitionen von C nach $X^{\not\models}$, da es sonst eine entsprechende Transition in M' gäbe und C' somit kei-

ne ergodische Menge von M' wäre. Das ist aber ein Widerspruch, da nämlich dann die Zustände von C zu $X^{\models}$ hinzugefügt worden wären.

□

Nun haben wir alles was wir brauchen, um zu zeigen, daß unsere Konstruktion den Wert der Wahrscheinlichkeit, daß M die Formel φ erfüllt, erhält.

Satz 3.1.

$$\mu(\mathbf{Y}_{\models\varphi}) = \mu'(\mathbf{Y}'_{\models\varphi'})$$

Beweis : Da M und M' auf den Erfülltmengen von LTL-Formeln über AP die gleiche Wahrscheinlichkeitsverteilung haben, folgt Gleichung 3.3, also

$$\mu(\mathbf{Y}_{\models\varphi}) = \mu'(\mathbf{Y}'_{\models\varphi}).$$

Weiterhin gilt mit Lemma 3.3 für alle Läufe von M' in jedem Schritt mit Wahrscheinlichkeit 1 $(\phi \mathcal{U} \psi \equiv \rho)$. Somit erhalten wir

$$\mu'(\mathbf{Y}'_{\models\varphi}) = \mu'(\mathbf{Y}'_{\models\varphi'}),$$

und der Beweis ist vollständig.

□

3.2 Konstruktion für den "Next Step"-Operator

Die Konstruktion zur Elimination eines "Next Step"-Operators geht analog zu der eben behandelten. Gegeben ein Probabilistisches Programm $\mathcal{T}_{prob} = (M, AP, L)$ und eine LTL-Formel φ über AP. Sei $X\phi$ eine "temporal innerste" Teilformel von φ, d. h. ϕ enthält keine temporalen Operatoren, besteht also nur aus atomaren Aussagen und Boolschen Operatoren. Auch hier werden wir ein neues Probabilistisches Programm $\mathcal{T}'_{prob}$ konstruieren, dessen Menge AP' der atomaren Aussagen aus AP und einer neuen atomaren Aussage ρ besteht. Sei φ' die Formel, die aus φ entsteht, indem man jedes Vorkommen von $X\phi$ durch ρ ersetzt. Es wird dann gelten:

$$\mu(\mathbf{Y}_{\models\varphi}) \;=\; \mu'(\mathbf{Y}'_{\models\varphi'}).$$

Zuerst werden wir wie gewohnt die Zustände des Probabilistischen Programms in drei disjunkte Mengen $X^{\models}, X^{\not\models}, X^{?}$ aufteilen. $X^{\models}$ wird die Zustände x enthalten, für die alle in x beginnenden echten Läufe die Formel $X\phi$ erfüllen. Entsprechend

wird $X^{\not\models}$ die Zustände x enthalten, für die alle in x beginnenden echten Läufe die Formel $X\phi$ erfüllen. In $X^?$ sind die Zustände x, für die ein in x beginnender Lauf die Formel $X\phi$ mit Wahrscheinlichkeit r, $0 < r < 1$ erfüllt. Da der "Next Step"-Operator eine lokale Eigenschaft beschreibt, ist diese Unterteilung sehr einfach.

- $X^{\models} = \{x \in X \mid (x,y) \in T \ \rightarrow \ y \models \phi\}$
- $X^{\not\models} = \{x \in X \mid (x,y) \in T \ \rightarrow \ y \not\models \phi\}$
- $X^? = \{x \in X \mid \exists (x,y_1),(x,y_2) \in T : y_1 \models \phi \ \wedge \ y_2 \not\models \phi\} \ = \ X \setminus (X^{\models} \cup X^{\not\models})$

Wie zuvor sei für $x \in X$ q_x die Wahrscheinlichkeit, daß ein in x beginnender Lauf die Formel $X\phi$ erfüllt. Also $q_x = \mu^x(\mathbf{Y}_{\models X\phi}) = \frac{\mu(\mathbf{Y}_{\models X\phi})}{p_0(x)}$. [13] Wie die Unterteilung von X ist die Berechnung der q_x aufgrund der Tatsache, daß der "Next Step"-Operator eine lokale Eigenschaft beschreibt auch sehr einfach. Offensichtlich gilt:

$$q_x \ = \ \sum_{\substack{y \in X \\ y \models \phi}} p_{xy} \ = \ \left\{ \begin{array}{rcl} 1 & : & x \in X^{\models} \\ 0 & : & x \in X^{\not\models} \\ \in (0,1) & : & x \in X^? \end{array} \right\} \tag{3.6}$$

Die Konstruktion

Die Konstruktion in diesem Fall ist sehr ähnlich zu der im vorigen Fall. Wir definieren uns ein neues Probabilistisches Programm $\mathcal{T}'_{prob} = (M', AP', L')$, wobei $AP' = AP \cup \rho$ mit $\rho \notin AP$. ρ wird hier für die Teilformel $X\phi$ stehen. Die Zustände von M' sind von der Form (x,ρ), falls $x \in X^{\models}$, $(x,\neg\rho)$, falls $x \in X^{\not\models}$ und $(x,\rho),(x,\neg\rho)$, falls $x \in X^?$. Ein Zustand (x,ρ) erfüllt dieselben atomaren Aussagen wie x und zusätzlich auch noch ρ. Ein Zustand $(x,\neg\rho)$ erfüllt nur dieselben atomaren Aussagen wie x. Die Transitionen und deren Wahrscheinlichkeiten werden so definiert, daß wir folgende Bedeutung erhalten. Die Wahrscheinlichkeit für einen in (x,ρ) beginnenden Lauf ist gleich der Wahrscheinlichkeit, daß ein in x beginnender Lauf $X\phi$ erfüllt. Genauer impliziert jede Transition (x,y) aus M ein oder zwei Transitionen in M'. Wir definieren die Transitionswahrscheinlichkeit für eine Transition $((x,\rho_1),(y,\rho_2)) \in T', \quad \rho_1,\rho_2 \in \{\rho,\neg\rho\}$ als die Wahrscheinlichkeit, daß für einen in x beginnender Lauf $Y = x,x_1,x_2,\ldots$ von M gilt, daß $x_1 = y$ und $x_1,x_2,\ldots$ erfüllt ρ_2 unter der Voraussetzung, daß $Y \ \ \rho_1$ erfüllt (wobei hier ρ für $X\phi$ und $\neg\rho$ für $\neg(X\phi)$ stehen). Formal sieht das so aus:

[13] siehe Bemerkung 4 auf Seite 18

Definition 3.2.1. Sei $\mathcal{T}'_{prob} = (M', AP', L')$ mit $M' = (X', T', p', p'_0)$ folgendes Probabilistische Programm.

- $AP' = AP \cup \{\rho\}, \;\; \rho \notin AP$
- $X' = \{(x,\rho) \mid x \in X^{\models} \cup X^{?}\} \quad \cup \quad \{(x,\neg\rho) \mid x \in X^{\not\models} \cup X^{?}\}$
- $L'(x,\rho) = L(x) \cup \{\rho\}$
  $L'(x,\neg\rho) = L(x)$
- $p'_0((x,\rho)) = p_0(x)q_x \quad \wedge \quad p'_0((x,\neg\rho)) = p_0(x)(1-q_x)$
- Im folgenden gelte $\rho_1, \rho_2 \in \{\rho, \neg\rho\}$. Sei T' die kleinste Teilmenge von T, die folgende Eigenschaften erfüllt: für alle $(x,y) \in T$ gilt
  - $x,y \in X^{\models} \cup X^{\not\models} \implies ((x,\rho_1),(y,\rho_2)) \in T'$
    Bemerke, daß nur eine Transition in T' eingefügt wird.
    Wir definieren $p'_{(x,\rho_1)(y,\rho_2)} = p_{xy}$.
  - $x \in X^{\models} \cup X^{\not\models} \;\wedge\; y \in X^{?} \implies ((x,\rho_1),(y,\rho))$ und $((x,\rho_1),(y,\neg\rho)) \in T'$
    Bemerke, daß ρ_1 eindeutig ist.
    Wir definieren $\begin{aligned} p'_{(x,\rho_1)(y,\rho)} &= p_{xy}q_y \\ p'_{(x,\rho_1)(y,\neg\rho)} &= p_{xy}(1-q_y). \end{aligned}$
  - $x \in X^{?} \;\wedge\; y \in X^{\models} \cup X^{\not\models}$:
    - $y \models \phi$
      $\implies ((x,\rho),(y,\rho_1)) \in T'$
      Bemerke, daß ρ_1 eindeutig ist.
      Wir definieren $p'_{(x,\rho)(y,\rho_1)} = \frac{p_{xy}}{q_x}$.
    - $y \not\models \phi$
      $\implies ((x,\neg\rho),(y,\rho_1)) \in T'$
      Wir definieren $p'_{(x,\neg\rho)(y,\rho_1)} = \frac{p_{xy}}{1-q_x}$.
  - $x,y \in X^{?}$:
    - $y \models \phi$
      $\implies ((x,\rho),(y,\rho))$ und $((x,\rho),(y,\neg\rho)) \in T'$
      Wir definieren $\begin{aligned} p'_{(x,\rho)(y,\rho)} &= p_{xy}\frac{q_y}{q_x} \\ p'_{(x,\rho)(y,\neg\rho)} &= p_{xy}\frac{1-q_y}{q_x}. \end{aligned}$

$*$ $y \not\models \phi$
$\Longrightarrow ((x,\neg\rho),(y,\rho))$ und $((x,\neg\rho),(y,\neg\rho)) \in T'$
Wir definieren $p'_{(x,\neg\rho)(y,\rho)} = p_{xy}\frac{q_y}{1-q_x}$
$p'_{(x,\neg\rho)(y,\neg\rho)} = p_{xy}\frac{1-q_y}{1-q_x}$.

■

Das weitere Vorgehen ist nun analog zu dem in Abschnitt 3.1. Sei also φ' diejenige Formel, die aus φ entsteht, indem alle Vorkommen von $X\phi$ durch ρ ersetzt werden. Auch in diesem Fall werden wir zeigen, daß

$$\mu(\mathbf{Y}_{\models\varphi}) \;=\; \mu'(\mathbf{Y}'_{\models\varphi'})$$

gelten wird, wobei μ' das Maß des Folgenraums von $\mathcal{T}'_{prob}$ ist. Dafür zeigen wir wie im Fall für den "Until"-Operator 2 Lemmata, aus denen die obige Gleichung leicht folgt.

Zuerst zeigen wir also, daß für eine messbare Teilmenge $A \subset X^\omega$ gilt :

$$\mu(A) = \mu'(\pi^{-1}(A)).^{14}$$

Es genügt jedoch, dies für alle Basiszylinder von M zu zeigen.[15]

Lemma 3.4. *Für alle $x_0, x_1, \ldots, x_n \in X, n \in \mathbb{N}$ gilt*

$$\mu(\Delta(x_0, x_1, \ldots, x_n)) = \mu'(\pi^{-1}(\Delta(x_0, x_1, \ldots, x_n))).$$

Beweis : Dieser Beweis geht analog zu dem Beweis von Lemma 3.2, Seite, 82 und wird hier nicht angegeben.

□

Mit der Aussage des Lemmas folgt nun insbesondere: für jede LTL-Formel $\tilde{\varphi}$ über AP gilt

$$\mu(\mathbf{Y}_{\models\tilde{\varphi}}) = \mu'(\mathbf{Y}'_{\models\tilde{\varphi}}).$$

Dies liegt daran, daß

$$\pi^{-1}(\mathbf{Y}_{\models\tilde{\varphi}}) = \mathbf{Y}'_{\models\tilde{\varphi}}.$$

Somit haben die Probabilistischen Systeme $\mathcal{T}_{prob}$ und $\mathcal{T}'_{prob}$ die gleiche Wahrscheinlichkeitsverteilung für LTL-Formeln über AP. Es gilt also auch

$$\mu(\mathbf{Y}_{\models\varphi}) = \mu'(\mathbf{Y}'_{\models\varphi}) \tag{3.7}$$

[14] Die Projektion π wurde in Abschnitt 3.1 aus Seite 82 definiert.
[15] Für detaillierte Erklärungen siehe [Bau78].

für die Formel φ aus unserer Konstruktion. Um die gewünschte Eigenschaft unserer Konstruktion nachzuweisen, müssen wir also noch zeigen, daß

$$\mu'(\mathbf{Y}'_{\models\varphi}) = \mu'(\mathbf{Y}'_{\models\varphi'})$$

gilt. Dies ist aber gewährleistet, wenn gilt

$$\mu'(\mathbf{Y}'_{\models X^k X\phi}) = \mu'(\mathbf{Y}'_{\models X^k\rho}) \quad \forall k \in \mathbb{N},$$

wenn also für alle $k \in \mathbb{N}$ und einen Lauf $Y' = x'_0, x'_1, x'_2, \ldots$ mit Wahrscheinlichkeit 1 gilt: $x'_k \models \rho$ gdw $x'_k, x'_{k+1}, \ldots \models X\phi$. Aufgrund der Tatsache, daß

$$\mathbf{Y}'_{\models X^k\tilde{\varphi}} = \bigcup_{x'_0,\ldots x'_{k-1}\in X'} \Delta'(x'_0,\ldots x'_{k-1})\mathbf{Y}'_{\models\tilde{\varphi}}$$

muss diese Eigenschaft nur für $k = 0$ gezeigt werden. Genau dies leistet das folgende Lemma.

Lemma 3.5.

$$\mu'(\mathbf{Y}'_{\models X\phi}) = \mu'(\mathbf{Y}'_{\models\rho})$$

Beweis : Dies folgt sehr einfach wie angegeben.

$$\mu'(\mathbf{Y}'_{\models\rho}) =$$

$$\mu'\left(\bigcup_{x\in X',x\models\rho}\Delta'(x)\right) =$$

$$\sum_{(x,\rho)\in X'} p'_0((x,\rho)) =$$

$$\sum_{x\in X^{\models}} p_0(x) + \sum_{x\in X^?} p_0(x)\cdot q_x \;=^{16}$$

$$\sum_{x\in X}\left(p_0(x)\cdot\sum_{y\in X,y\models\phi} p_{xy}\right)$$

$$\mu(\mathbf{Y}_{\models X\phi}) =^{17}$$

$$\mu'(\mathbf{Y}'_{\models X\phi}).$$

□

[16] Siehe Gleichung 3.6, Seite 89, aus der folgt: $q_x = \sum_{y\in X,y\models\phi} p_{xy} = 1$, bzw. 0, falls $x \in X^{\models}$, bzw. $x \in X^{\not\models}$.

[17] wegen Lemma 3.4

Nun haben wir alles was wir brauchen, um zu zeigen, daß unsere Konstruktion den Wert der Wahrscheinlichkeit, daß M die Formel φ erfüllt, erhält.

Satz 3.2.

$$\mu(\mathbf{Y}_{\models\varphi}) = \mu'(\mathbf{Y}'_{\models\varphi'})$$

Beweis : Da M und M' auf den Erfülltmengen von LTL-Formeln über AP die gleiche Wahrscheinlichkeitsverteilung haben, folgt Gleichung 3.7, also

$$\mu(\mathbf{Y}_{\models\varphi}) = \mu'(\mathbf{Y}'_{\models\varphi}).$$

Weiterhin gilt mit Lemma 3.5 für alle Läufe von M' in jedem Schritt mit Wahrscheinlichkeit 1 $(X\phi \equiv \rho)$. Somit erhalten wir

$$\mu'(\mathbf{Y}'_{\models\varphi}) = \mu'(\mathbf{Y}'_{\models\varphi'}),$$

und der Beweis ist vollständig.

□

Wir haben also gesehen, wie man schrittweise die temporalen Operatoren aus der Formel φ entfernen kann.

3.3 Der Algorithmus

Bevor wir nun den diesem Vorgehen entsprechenden Algorithmus zur Berechnung von $\mu(\mathbf{Y}_{\models\varphi})$ angeben, folgt noch eine Definition.

Definition 3.3.1.
Gegeben ein Probabilistisches Programm $\mathcal{T}_{prob} = (M, AP, L)$ und eine LTL-Formel φ über AP. Sei ψ eine temporal innerste Teilformel von φ, d. h. ψ enthalte genau einen temporalen Operator. Falls nun ψ einen "Next Step"-Operator enthält, dann bezeichne

$$T_\psi(\mathcal{T}_{prob})$$

das in Abschnitt 3.2 konstruierte Probabilistische Programm $\mathcal{T}'_{prob}$ aus Definition 3.2.1, Seite 90 und

$$T_\psi(\varphi)$$

die dazugehörige in Abschnitt 3.2 aus φ konstruierte LTL-Formel φ'.

Falls aber ψ einen "Until"-Operator enthält, dann bezeichne

$$T_\psi(\mathcal{T}_{prob})$$

das in Abschnitt 3.1 konstruierte Probabilistische Programm $\mathcal{T}'_{prob}$ aus Definition 3.1.1, Seite 80 und

$$T_\psi(\varphi)$$

die dazugehörige in Abschnitt 3.1 aus φ konstruierte LTL-Formel φ'. ■

Algorithmus 2 Grundidee eines quantitativen probabilistischen Modelchecking Algorithmus ohne *Buechi*-Automaten

---

- Eingabe : gegeben sei ein Probabilistisches Programm $\mathcal{T}^0_{prob} = (M, AP, L)$ und eine LTL-Formel φ^0 über AP
- Ausgabe : ausgegeben wird der Wert $\mu(\mathbf{Y}_{\models\varphi^0})$

---

sei k die Anzahl an temporalen Operatoren von φ^0;
FOR $i = 1, 2, \ldots, k$ **DO**
  sei ψ eine temporal innerste Teilformel von φ^{i-1}
  $\mathcal{T}^i_{prob} = T_\psi(\mathcal{T}^{i-1}_{prob})$
  $\varphi^i = T_\psi(\varphi^{i-1})$
OD
(*φ^k enthält also keine temporalen Operatoren*)
berechne die Menge A der Zustände von $\mathcal{T}^k_{prob}$, die φ^k erfüllen;
gib den Wert $\sum_{x\in A} p^k_0(x)$ aus;

Die Korrektheit des angegebenen Algorithmus folgt sofort aus Satz 3.1, Seite 88 und Satz 3.2, Seite 93.

Wir wollen uns jetzt Gedanken zur Laufzeit des Algorithmus machen. Wenn k die Anzahl an temporalen Operatoren der Formel φ^0 ist, so wird der Algorithmus also k-mal entweder die Konstruktion aus Abschnitt 3.1 oder Abschnitt 3.2 durchführen. Aus diesen Abschnitten wissen wir, daß

$$|\mathcal{T}^i_{prob}| \leq 2 \cdot |\mathcal{T}^{i-1}_{prob}|, \quad i = 1, 2, \ldots, k$$

gilt (siehe Definitionen 3.1.1 und 3.2.1). Somit gilt

$$|\mathcal{T}^k_{prob}| \leq 2^k \cdot |\mathcal{T}^0_{prob}|.$$

Betrachten wir jetzt die Laufzeit eines Konstruktionsschritts. Wir werden hier nur die Konstruktion für den "Until"-Operator betrachten. Bemerke, daß die Konstruktion für den "Next Step"-Operator einfacher ist und auch weniger Laufzeit benötigt. Sei also $\phi \mathcal{U} \psi$ die Teilformel von φ, die eliminiert werden soll.[18] Als erstes werden die Zustände des gegebenen Probabilistischen Programs $\mathcal{T}_{prob}$ in drei disjunkte Mengen $X^{\models}$, $X^{\not\models}$, $X^{?}$ aufgeteilt. Dies geschieht wie folgt : (siehe Algorithmus 3, Seite 96)

Daß der Algorithmus korrekt arbeitet, ist relativ einfach zu sehen. Man beachte, daß die starken Zusammenhangskomponenten von H in ihrer umgekehrten topologischen Reihenfolge bearbeitet werden, d. h. , wenn die Knoten einer SCC bearbeitet werden, so sind alle ihre Nachfolger schon zu $X^{\models}$ oder $X^{\not\models}$ oder $X^{?}$ zugeteilt worden.

Sei $t = |\phi \mathcal{U} \psi|$. Wir bemerken nun, daß die Mengen X_ϕ und X_ψ in Zeit $O(t \cdot |\mathcal{T}|)$ berechnet werden können. Die SCCs von H können linear in der Größe von H berechnet werden (siehe [JU94]), also auf jeden Fall in Zeit $O(|\mathcal{T}|)$.

Da nach der Berechnung der Mengen $X^{\models}$, $X^{\not\models}$ und $X^{?}$ die Konstruktion des neuen Graphen nur noch linear in $|\mathcal{T}_{prob}|$ ist, folgt : der Graph von $\mathcal{T}^i_{prob}$ kann also aus dem Graphen von $\mathcal{T}^{i-1}_{prob}$ in Zeit $O(t_{i-1} \cdot |\mathcal{T}^{i-1}_{prob}|)$ konstruiert werden, wobei $t_i = |\varphi_i|$. Da nun

$$|\mathcal{T}^i_{prob}| \leq 2^i \cdot |\mathcal{T}^0_{prob}|$$

folgt durch Aufsummieren des Zeitaufwands für jeden Schritt, daß der Graph von $\mathcal{T}^k_{prob}$ aus dem Graphen von $\mathcal{T}^0_{prob}$ in Zeit

$$O(t \cdot 2^k \cdot |\mathcal{T}^0_{prob}|)$$

mit $t = max_{i=0,1,\ldots,(k-1)} t_i$ konstruiert werden kann. Mit $t + k \leq |\varphi| + 1$ folgt : Der Graph von $\mathcal{T}^k_{prob}$ kann aus dem Graphen von $\mathcal{T}^0_{prob}$ in Zeit

$$O(2^{|\varphi|} \cdot |\mathcal{T}^0_{prob}|)$$

konstruiert werden.

Daraus folgt, daß man qualitatives LTL-Model Checking in Zeit

$$O(2^{|\varphi|} \cdot |\mathcal{T}^0_{prob}|)$$

[18] Beachte, daß ϕ und ψ aussagenlogische Formeln über der Menge der atomaren Aussagen des gegebenen Probabilistischen Programms sind.

Algorithmus 3

- Eingabe : gegeben sei ein Probabilistisches Programm $\mathcal{T}_{prob} = (M, AP, L)$ und eine LTL-Formel $\phi \mathcal{U} \psi$, wobei ϕ und ψ keine temporalen Operatoren enthalten
- Ausgabe : ausgegeben werden die Mengen $X^{\models}$, $X^{\not\models}$, $X^{?}$, die wie in Abschnitt 3.1 definiert sind

---

$X^{\models} = X^{\not\models} = X^{?} = \emptyset$;
berechne $X_\phi = \{x \in X : x \models \phi\}$;
berechne $X_\psi = \{x \in X : x \models \psi\}$;
$X^{\models} = X_\psi$
$X^{\not\models} = X \setminus (X_\phi \cup X_\psi)$
(* sei H der Teilgraph des zugrundeliegenden Graphen von $\mathcal{T}_{prob}$, der von der Zustandsmenge $X_\phi \setminus X_\psi$ induziert wird *)
berechne die starken Zusammenhangskomponenten (SCCs) $C_1, \ldots, C_n$ von H und ordne diese topologisch;
(* sei $C_{i_1}, \ldots, C_{i_n}$ eine topologische Sortierung *)
FOR $j = n, (n-1), \ldots, 1$ **DO**
  IF alle Kanten, die aus C_{i_j} hinausführen, führen nach $X^{\not\models}$ **THEN**
    $X^{\not\models} = X^{\not\models} \cup C_{i_j}$;
  ELSE
    IF alle Kanten, die aus C_{i_j} hinausführen, führen nach $X^{\models}$ und es gibt mindestens eine solche Kante **THEN**
      $X^{\models} = X^{\models} \cup C_{i_j}$;
    ELSE
      $X^{?} = X^{?} \cup C_{i_j}$;
    FI
  FI
  $H = H \setminus C_{i_j}$;
  (* entferne also alle Zustände von C_{i_j} und damit inzidente Kanten aus H *)
OD
gib $X^{\models}$, $X^{\not\models}$, $X^{?}$ aus;

---

durchführen kann (man muss nach der Konstruktion des Graphen von $\mathcal{T}^k_{prob}$ nur noch überprüfen, ob alle Anfangszustände die aussagenlogische Formel φ^k erfüllen.

Wie hoch ist der Aufwand beim quantitativen LTL-Model Checking? Dazu müssen wir in jedem Schritt neben dem Graphen von $\mathcal{T}^i_{prob}$ auch noch die Transitionswahrscheinlichkeiten von $\mathcal{T}^i_{prob}$ ausrechnen. Wir haben gesehen, daß wir diese im Falle der Konstruktion für den "Until"-Operator durch Lösen eines linearen Gleichungssystems in der Größe der Anzahl der Knoten von $\mathcal{T}^{i-1}_{prob}$ erhalten können.[19] Dies bedeutet, daß in jedem Schritt noch ein Aufwand von $O(poly(|\mathcal{T}^{i-1}_{prob}|))$ hinzukommt, was dazu führt, daß man den Gesamtaufwand zum erstellen von $\mathcal{T}^k_{prob}$ aus $\mathcal{T}^0_{prob}$ durch

$$O(2^{O(|\varphi^0|)} \cdot poly(|\mathcal{T}^0_{prob}|))$$

abschätzen kann. Das berechnen der Menge A und des Wertes $\sum_{x\in A} p^k_0(x)$ fällt dann nicht mehr ins Gewicht.

Es gilt also, daß wir den Wert

$$\mu(\mathbf{Y}_{\models\varphi^0})$$

mit einem Zeitaufwand berechnen können, der exponentiell in der Länge der Formel φ^0 ist und polynomiell in der Größe des Systems $\mathcal{T}^0_{prob}$.

Zusammenfassend kann man also sagen, daß die Zeitkomplexität der Methode ohne *Buechi*-Automaten nur einfach exponentiell in der Formellänge ist, während die Zeitkomplexität der Methode mit *Buechi*-Automaten doppelt exponentiell in der Formellänge ist. Die Zeitkomplexität beider Methoden ist zudem polynomiell in der Größe des gegebenen Systems.

[19] Bemerke, daß wir die Transitionswahrscheinlichkeiten im Falle der Konstruktion für den "Next Step"-Operator sofort angeben konnten.

Literaturverzeichnis

[Bau78] H. Bauer: *Wahrscheinlichkeitstheorie und Grundzüge der Maßtheorie*, de Gruyter, 1978 (3. Auflage)

[BCM+92] J. R. Burch, E. M. Clarke, K. L. McMillan, D. L. Dill, L. J. Hwang: Symbolic Model Checking: 10^{20} states and beyond, *Information and Computation 98(2)*, pp 142-170, 1992

[ClEm81] E. Clarke, E.A. Emerson: Design and Synthesis of Synchronization Skeletons from Branching Time Temporal Logic, Proc. Workshop on Logics of Programs, *Lecture Notes in Computer Science*, Vol. 131, pp 52-71, 1981.

[CGP00] E. Clarke, O. Grumberg, D. Peled: *Model Checking*, MIT Press, 2000.

[CoYa88] C. Courcoubetis, M. Yannakakis: Verifying Temporal Properties of Finite-State Probabilistic Programs, *Proc. 29th Annual Symp. on Foundations of Computer Science*, pp 338-345, 1988.

[CoYa95] C. Courcoubetis, M. Yannakakis: The Complexity of Probabilistic Verification, *Journal of the ACM*, Vol. 42, No. 4, pp 857-907, 1995.

[EtHo00] K. Etessami, G. J. Holzmann: Optimizing Büchi automata, *Proc. 11th International Conference on Concurrency Theory (CONCUR2000)*, pp 153-167. Springer, 2000. LNCS 1877.

[JU94] D. Jungnickel: *Graphen, Netzwerke und Algorithmen*, BI-Wissenschaftsverlag, 1994

[KS60] J. G. Kemeny, J. L. Snell: *Finite Markov Chains*, Van Nostrad, Princeton, 1960.

[KSK76] J. G. Kemeny, J. L. Snell, A. W. Knapp: *Denumerable Markov Chains*, Springer-Verlag, New York, 1976.

[McMi93] K. L. McMillan: *Symbolic Model Checking: An Approach to the State Explosion Problem*, Kluwer Academic, 1993

[Pnue77] A. Pnueli: The Temporal Logic of Programs, Proc. FOCS'77, pp 46-57, 1977.

[SoBl00] F. Somenzi, R. Bloem: Efficient Büchi Automata from LTL Formulae, *Proceedings of 12th Int. Conf. on Computer Aided Verification*, pp 247-263. Springer Verlag, 2000. LNCS 1633

[Va85] M. Vardi: Automatic verification of probabilistic concurrent finite-state programs., *Proceedings of 26th IEEE Symposium on Foundations of Computer Science*, IEEE, New York, 1985, pp 327-338.

[WVS83] P. Wolper, M. Vardi, A. Sistla: Reasoning about infinite computation paths, *Proceedings of the 24th IEEE Symposium on Foundations of Computer Science*, IEEE, New York, pp. 185-194, 1983