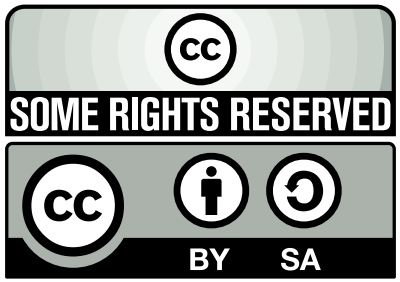
Temporale Logik und Bisimulation

Julian Fietkau, Nils Kubera, Dominik Nuszpl

Universität Hamburg

2. Februar 2011

Organisatorisches vorweg



Folien-Download und Feedback-Möglichkeit:

`http://www.julian-fietkau.de/temporale_logik_und_bisimulation`

Übersicht

Einleitung

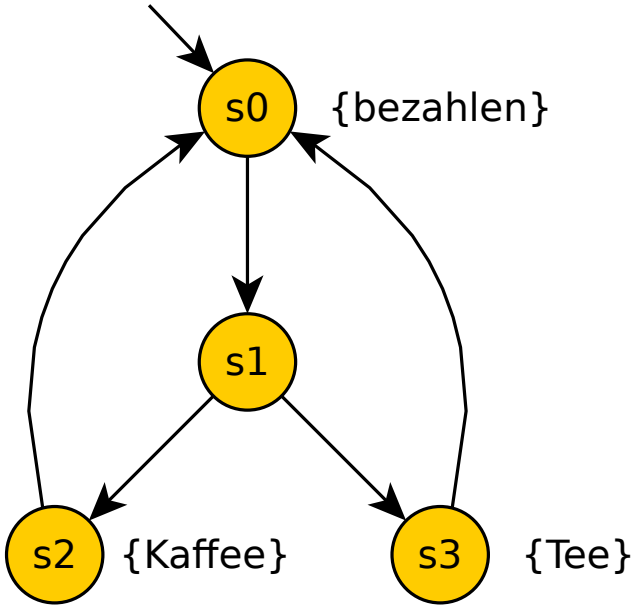
Wir betrachten **Transitionssysteme** als Werkzeug zur Spezifikation und Modellierung.

Definition 1: Transitionssystem

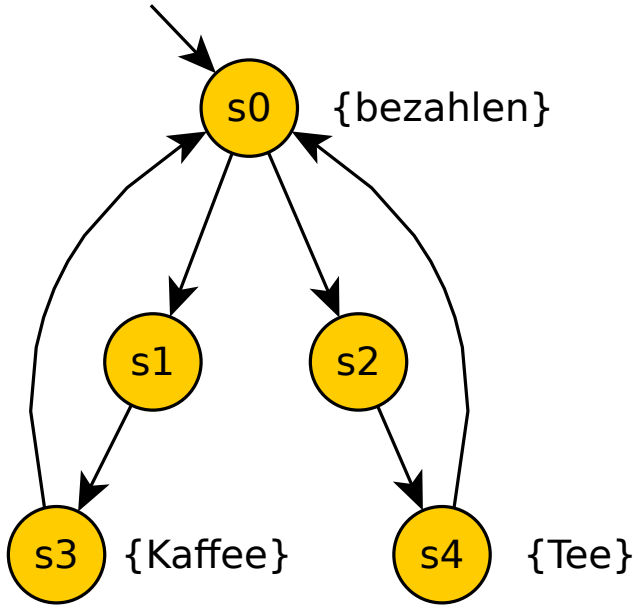
$TS = (S, A, tr, S^0, S^F)$
Im Folgenden meist vereinfacht verwendet: $TS = (S, A, tr, s^0)$ (Nur ein Startzustand, keine Endzustände)

Um Gesetzmäßigkeiten im Verhalten verschiedener Transitionssysteme erkennen und beschreiben zu können, untersuchen wir verschiedene Arten der Äquivalenz, nämlich **Folgenäquivalenz** und **Bisimulation**.

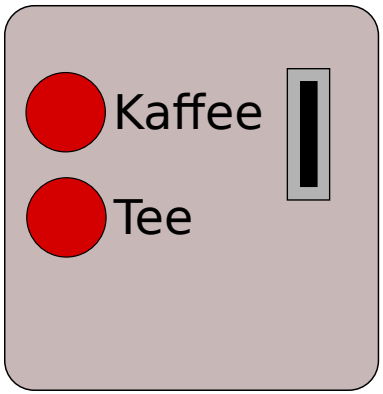
Kaffee oder Tee?

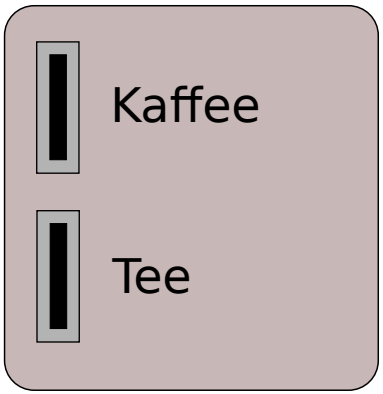


TS_1



TS_2





Gemeinsame Zustandsfolgen

Welche Zustandsfolgen sind in den Transitionssystemen möglich?

$w_1 = (\mathit{bezahlen}, \mathit{Kaffee}, \mathit{bezahlen}, \mathit{Kaffee}, \mathit{bezahlen}, \mathit{Tee})$

$w_2 = (\mathit{bezahlen}, \mathit{Tee}, \mathit{bezahlen}, \mathit{Tee}, \mathit{bezahlen}, \mathit{Tee}, \ldots)$

Behauptung: Jede Folge, die in TS_1 möglich ist, ist auch in TS_2 möglich und umgekehrt. Die beiden Transisionssysteme sind **folgenäquivalent**.

(Der Beweis bleibt dem Leser zur Übung überlassen.)

Bedeutet das, dass die beiden TS in jeder Hinsicht gleich sind? **Nein!** Wir können sinnvolle Äquivalenzkriterien finden, nach denen sie verschieden sind.

Definition

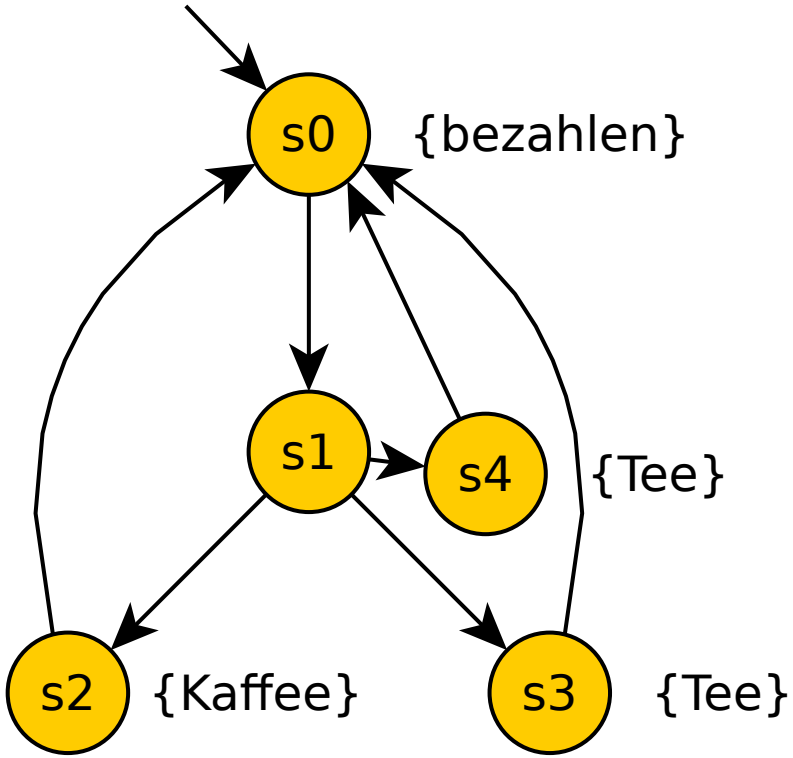
Definition 2: (Zustandsbasierte) Bisimulation

$TS_1 = (S_1, A, tr_1, S_1^0)$ und $TS_2 = (S_2, A, tr_2, S_2^0)$ sind bisimilar genau dann, wenn eine binäre Relation („Bisimulation“) $\mathcal{B} \subseteq S_1 \times S_2$ existiert, so dass gilt:

1. $\forall s_0 \in S_1^0 \; \exists r_0 \in S_2^0 : (s_0, r_0) \in \mathcal{B}$
   $\forall r_0 \in S_2^0 \; \exists s_0 \in S_1^0 : (s_0, r_0) \in \mathcal{B}$
2. Für alle $(r_1, s_1) \in \mathcal{B}$ gilt:
   $r_2 \in Post(r_1) \Rightarrow \exists s_2 \in Post(s_1) : (r_2, s_2) \in \mathcal{B}$
   $s_2 \in Post(s_1) \Rightarrow \exists r_2 \in Post(r_1) : (r_2, s_2) \in \mathcal{B}$
   $L(r_1) = L(s_1)$

Hierbei ist L eine Etikettierungsfunktion, die den (relevanten) Zuständen Bezeichnungen zuordnet. $Post(s)$ ist die Menge der von s aus direkt erreichbaren Nachfolgezustände.

Ein Beispiel



TS_3

TS_1 und TS_3 sind bisimilar.

Kaffee oder Tee? – eine genauere Analyse

Betrachte TS_1 und TS_2:

1. $(s_0, s_0') \in \mathcal{B}$, erste Teilbedingung ist damit erfüllt.
2. Nun muss weiterhin gelten: $(s_1, s_i') \in \mathcal{B}$ mit $i \in \{1, 2\}$ (Nachfolger von s_0')
3. Da $s_3 \in Post(s_1)$ und $(s_1, s_1') \in \mathcal{B}$ und $s_3' \in Post(s_1')$ mit $|Post(s_1')| = 1$, folgt zwangsweise: $(s_3, s_3') \in \mathcal{B}$
4. Jedoch ist $L(s_3) \neq L(s_3')$ ↯

TS_1 und TS_2 sind nicht bisimilar.

Fazit

- Folgenäquivalenz macht Aussagen über das Verhalten der Systeme von außen betrachtet. Bisimulation beschreibt zusätzlich die interne Struktur.
- Bisimulation impliziert automatisch auch Folgenäquivalenz:
  $TS_a \sim TS_b \Rightarrow TS_a \equiv_{trace} TS_b$
  $(TS_a \equiv_{trace} TS_b \not\Rightarrow TS_a \sim TS_b)$
  - Systeme, die die gleichen Zustandsfolgen erlauben, sind nicht unbedingt verhaltensäquivalent.

LTL

- $\bigcirc\varphi$: nächster Zustand erfüllt φ
  $\Diamond\varphi$: irgendein Folgezustand erfüllt φ
  $\Box\varphi$: alle folgenden Zustände erfüllen φ
  $\varphi_1 \cup \varphi_2$: φ_1 gilt bis in einem Folgezustand φ_2 erfüllt ist
- LTL Formeln

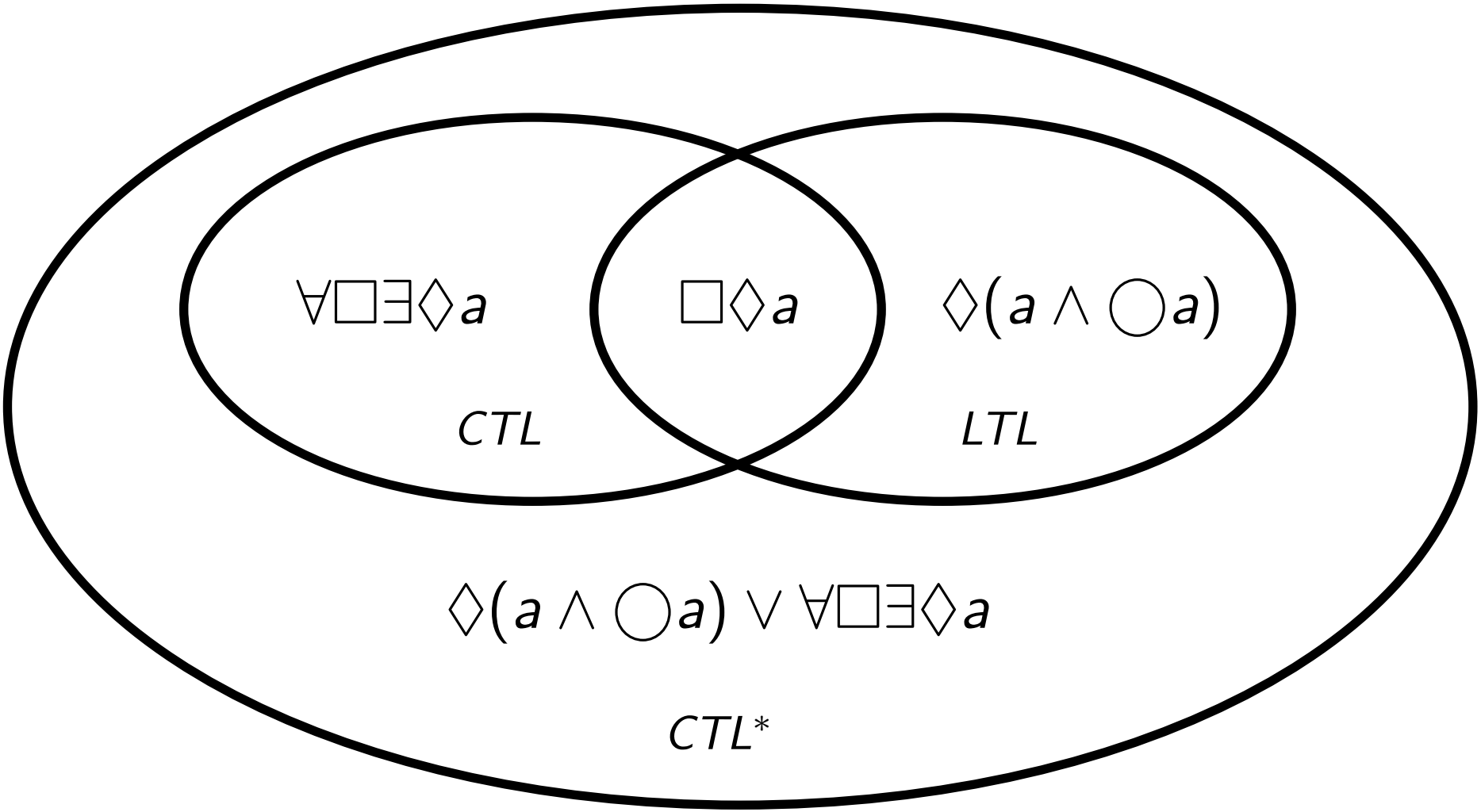
Definition 3: LTL-Formeln

$\varphi \equiv \mathit{true} \mid \mathit{false} \mid a \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \Diamond\varphi \mid \Box\varphi \mid \varphi_1 \cup \varphi_2$

CTL und CTL*

- zusätzlich Zustandsformeln mit Quantoren, die sich auf alle vom Zustand ausgehenden Pfade beziehen
- Quantoren
  - $\forall\varphi$: entlang aller Pfade gilt φ
  - $\exists\varphi$: entlang mindestens eines Pfads gilt φ
- CTL ist eine Teilmenge von CTL*.
- Jeder Temporaloperator wird durch genau einen Pfadquantor quantifiziert.
  - $\exists \bigcirc \varphi$: in mind. einem nächsten Zustand gilt φ
  - $\exists\Diamond\varphi$: in mind. einem der folgenden Zustände gilt φ
  - $\exists\Box\varphi$: es gibt mind. einen Pfad, in dem φ entlang des kompletten Pfades gilt
  - ...
  - $\forall \bigcirc \varphi$: in jedem nächsten Zustand gilt φ
  - ...

Verhältnis zwischen LTL, CTL und *CTL**



Gültigkeit für CTL*-Zustandsformeln

Sei $TS := (S, Act, \rightarrow, I, AP, L)$ ein Transitionssystem ohne Endzustände, s $\in$ S ein Zustand, Φ und Ψ CTL*-Zustandsformeln und φ,φ_1 und φ_2 CTL*-Pfadformeln.

Definition 4: Gültigkeit von Zustandsformeln

Die Gültigkeit $\models$ für CTL*-Zustandsformeln wird definiert durch

- $s \models a \Leftrightarrow a \in L(s)$,
- $s \models \neg\Phi \Leftrightarrow$ not s $\models \Phi$,
- $s \models \Phi \wedge \Psi \Leftrightarrow (s \models \Phi)$ and $(s \models \Psi)$,
- $s \models \exists\varphi \Leftrightarrow \pi \models \varphi$ für mind. einen Pfad beginnend in s,
- $s \models \forall\varphi \Leftrightarrow \pi \models \varphi$ für alle Pfade beginnend in s

Gültigkeit für CTL*-Pfadformeln

Sei $\pi = s_0 s_1 s_2 \ldots$ ein Pfad und $\pi[i..]$ mit $i \geq 0$ ein Teilpfad von π beginnend bei Index i.

Definition 5: Gültigkeit von Pfadformeln

Die Gültigkeit $\models$ für CTL*-Pfadformeln wird definiert durch

- $\pi \models \Phi \Leftrightarrow s_0 \models \Phi$,
- $\pi \models \varphi_1 \wedge \varphi_2 \Leftrightarrow \pi \models \varphi_1$ and $\pi \models \varphi_2$,
- $\pi \models \neg\varphi \Leftrightarrow \pi \not\models \varphi$,
- $\pi \models \bigcirc\varphi \Leftrightarrow \pi[1..] \models \varphi$,
- $\pi \models \varphi_1 \cup \varphi_2 \Leftrightarrow \exists j \geq 0.(\pi[j..] \models \varphi_2 \wedge (\forall 0 \leq k < j.\pi[k..] \models \varphi_1))$,

CTL*-Äquivalenz in Transitionssystemen

Seien TS, TS_1 und TS_2 Transitionssysteme ohne Endzustände.

Definition 6: $\equiv_{CTL^*}$ für Zustände

Für Zustände s_1, s_2 in TS gilt:
$s_1 \equiv_{CTL^*} s_2$, wenn
$s_1 \models \Phi \Leftrightarrow s_2 \models \Phi$ für alle CTL*-Zustandfomeln Φ über AP.

Definition 7: $\equiv_{CTL^*}$ für Transitionssysteme

Für TS_1, TS_2 gilt:
$TS_1 \equiv_{CTL^*} TS_2$, wenn
$TS_1 \models \Phi \Leftrightarrow TS_2 \models \Phi$ für alle CTL*-Zustandfomeln Φ über AP.

Folgenäquivalenz $\subseteq$ LTL-Äquivalenz

- Zu zeigen: $\equiv_{trace} \subseteq \equiv_{LTL}$
- Sei TS ein Transitionssystem ohne Endzustände und s_1, s_2 Zustände in TS.
- Wenn $s_1 \not\equiv_{CTL} s_2$, existiert eine CTL-Zustandsformel Φ mit $s_1 \models \Phi$ und $s_2 \not\models \Phi$.
- Dies gilt analog für CTL*, aber nicht für LTL.

Beweis: Folgenäquivalenz $\subseteq$ LTL-Äquivalenz

Angenommen $s_1 \not\equiv_{LTL} s_2$ und Folgen(s_1) ist eine echte Teilmenge von Folgen(s_2). Dann gelten alle LTL Formeln, die für s_2 gelten, ebenso für s_1. Da jedoch in Folgen(s_2) Folgen enthalten sind, die nicht in Folgen(s_1) existieren, gibt es eine LTL-Formel φ mit $s_2 \models \varphi$ aber $s_1 \not\models \varphi$. ■

Äquivalenzrelationen für Transitionssysteme

Zu Zeigen für endliche Transitionssysteme ohne Endzustände:

$$\equiv_{CTL^*} = \equiv_{CTL} = \sim_{TS}$$

- Beweis in drei Schritten.

Die feiner/gröber-Beziehung

Seien $\sim_a$ und $\sim_b$ Äquivalenzrelationen über der gleichen Menge S.

Definition 8: feiner/gröber-Beziehung

$\sim_a$ ist feiner als $\sim_b$, wenn für alle $s_1, s_2 \in S$ gilt:
$s_1 \sim_a s_2 \Rightarrow s_1 \sim_b s_2$.
Geschrieben $\sim_a \subseteq \sim_b$.

$\equiv_{CTL^*}$ ist feiner als $\equiv_{CTL}$

Für $s_1, s_2 \in S$:

Beweis: $\equiv_{CTL^*} \subseteq \equiv_{CTL}$

Zu Zeigen:

$$s_1 \equiv_{CTL*} s_2 \Rightarrow s_1 \equiv_{CTL} s_2$$

Gibt es keine Formel Φ in CTL^* mit $s_1 \models \Phi$ und $s_2 \not\models \Phi$ (oder umgekehrt), so kann es auch keine in CTL geben, da $CTL \subseteq CTL^*$.
Entspricht $\neg(s_1 \equiv_{CTL^*} s_2 \wedge \neg(s_1 \equiv_{CTL} s_2))$ was äquivalent zur Vermutung ist.
Es folgt nach Definition 8:
$\equiv_{CTL^*} \subseteq \equiv_{CTL}$ ■

$\equiv_{CTL}$ ist feiner als $\sim_{TS}$

Zu Zeigen: $s_1 \equiv_{CTL} s_2 \Rightarrow s_1 \sim_{TS} s_2$

Beweiskonzept: $\equiv_{CTL} \subseteq \sim_{TS}$

- Relation $R = \{(s_1, s_2) \in S \times S | s_1 \equiv_{CTL} s_2\}$
- Damit die Annahme gilt, muss R die Punkte 1 – 3 der Definition 2.2 erfüllen.
- Punkt 1: Da Label $L(s)$ die atomaren Formeln darstellen, müssen CTL-äquivalente Formeln die gleichen Label besitzen. $L(s_1) = L(s_2)$.
- Punkt 2 und 3: Gilt für Formelmenge Ψ:
  $s_1' \models \Psi$ dann gilt $s_1 \models \exists \bigcirc \Psi$. Da $(s_1, s_2) \in R$ gilt $s_2 \models \exists \bigcirc \Psi$ und es gibt ein $s_2' \models \Psi$, womit $(s_1', s_2') \in R$. ■

$\sim_{TS}$ ist feiner als $\equiv_{CTL^*}$

Zu Zeigen: $s_1 \sim_{TS} s_2 \Rightarrow s_1 \equiv_{CTL^*} s_2$

Beweiskonzept: $\sim_{TS} \subseteq \equiv_{CTL^*}$

Seien s_1, s_2 Zustände in TS, π_1, π_2 unendliche Teilpfade
Zu Zeigen:

a Wenn $s_1 \sim_{TS} s_2$, dann gilt für jede CTL* Formel $\Phi : s_1 \models \Phi \Leftrightarrow s_2 \models \Phi$

b Wenn $\pi_1 \sim_{TS} \pi_2$, dann gilt für jede CTL* Pfad-Formel $\gamma : \pi_1 \models \gamma \Leftrightarrow \pi_2 \models \gamma$

Beweis erfolgt per Induktion über Formelstruktur.

Induktionsbeweis $\sim_{TS}$ ist feiner als $\equiv_{CTL^*}$ (1)

Es gelte: $s_1 \sim_{TS} s_2$.
(a) Induktionsbasis:
Für $\Phi = \mathit{true}$ gilt Annahme a.
Da $L(s_1) = L(s_2)$ gilt, gilt für $\Phi = a \in AP$:

$$s_1 \models a \Leftrightarrow a \in L(s_1) \Leftrightarrow a \in L(s_2) \Leftrightarrow s_2 \models a$$

Induktionsschritt:

1. $\Phi = \Phi_1 \wedge \Phi_2$.

$$s_1 \models \Phi_1 \wedge \Phi_2 \Leftrightarrow s_1 \models \Phi_1 \text{ and } s_1 \models \Phi_2$$
$$\Leftrightarrow s_2 \models \Phi_1 \text{ and } s_2 \models \Phi_2 \Leftrightarrow s_2 \models \Phi_1 \wedge \Phi_2$$

2. $\Phi = \neg\Psi$.

$$s_1 \models \neg\Psi \Leftrightarrow s_1 \not\models \Psi$$
$$\Leftrightarrow s_2 \not\models \Psi \Leftrightarrow s_2 \models \neg\Psi$$

Induktionsbeweis $\sim_{TS}$ ist feiner als $\equiv_{CTL^*}$ (2)

3 $\Phi = \exists\gamma$. Es reicht zu zeigen:

$$s_1 \models \exists\gamma \Longrightarrow s_2 \models \exists\gamma$$

Lässt sich über Pfadeigenschaften der Bisimulation zeigen.

(b) Induktion über Pfade entsprechend für die Formeln:

$$\gamma = \Phi, \gamma = \gamma_1 \wedge \gamma_2, \gamma = \neg\psi, \gamma = \bigcirc\psi, \gamma = \gamma_1 U \gamma_2$$

Da gilt:

$$\sim_{TS} \quad \subseteq \quad \equiv_{CTL^*} \quad \subseteq \quad \equiv_{CTL} \quad \subseteq \quad \sim_{TS}$$

gilt:

$$\equiv_{CTL^*} \quad = \quad \equiv_{CTL} \quad = \quad \sim_{TS}$$

Was bedeutet: Bisimilare Transitionssysteme erfüllen die gleichen CTL*- und CTL-Formeln.

Beispiel

$TS_1 \not\sim_{TS} TS_2$, $TS_1 \sim_{TS} TS_3$

	TS_1	TS_2	TS_3
$\exists \bigcirc (\exists \bigcirc Kaffee \wedge \exists \bigcirc Tee)$	$\surd$	$\times$	$\surd$
$\neg\exists \bigcirc (\exists \bigcirc Kaffee \wedge \exists \bigcirc Tee)$	$\times$	$\surd$	$\times$
$\exists \bigcirc (\exists \bigcirc Kaffee \vee \exists \bigcirc Tee)$	$\surd$	$\surd$	$\surd$

Fazit

- Es existieren verschiedene Äquivalenzrelationen für Transitionssysteme, wie Folgenäquivalenz, Bisimulation, $\equiv_{LTL}$, $\equiv_{CTL}$, $\equiv_{CTL^*}$, die teilweise äquivalent zueinander sind.
- Diese Äquivalenzen lassen sich beispielsweise beim Model Checking einsetzen, um die Komplexität zu verringern.
  (Bsp.: Formel Φ wird in Bisimulationsquotient von TS nicht erfüllt $\rightarrow TS \not\models \Phi$.)

Ende

Danke für die Aufmerksamkeit!