Kapitel II

Temporallogik und Model Checking

Inhalt Kapitel II

- Einführung
- Die Temporallogik CTL
  - Syntax und informelle Semantik
  - Semantik
  - Äquivalenzen
- CTL-Model Checking
  - Labelling Algorithmus
  - Optimierungen
- Das System SMV
- Fairness
- Das Alternating Bit Protokoll
- Symbolisches Model-Checking
- Bounded Model-Checking

Motivation

Unter *Model Checking* versteht man die automatische Überprüfung, ob ein Systemmodell eine Spezifikation erfüllt.

Die Modellierungen nebenläufiger Systeme aus Kapitel 1 waren bereits Beispiel dafür:

- Die Modellierungen mit SAT-Solvern sind Instanzen von *Bounded Model Checking* (da die Simulationszeit beschränkt ist).
- Die Modellierungen mit BDDs sind Instanzen von *Symbolic Model Checking* (da Zustandsmengen nicht explizit, sondern “symbolisch” repräsentiert wurden)

Arten von Eigenschaften

Typische Arten von spezifizierten Eigenschaften:

- **Safety**: System gerät in keinen “verbotenen” Zustand / alle erreichbaren Zustände sind “erlaubt” (hatten wir schon).
- **Liveness**: System verklemmt sich nicht; “Reset-Zustand” von überall ereichbar; jede “Anfrage” wird irgendwann “beantwortet”.
- **Fairness**: bestimmte “gute Eigenschaft” gilt für alle “fairen” Abläufe.

Diese Klassifikation erfasst die meisten Eigenschaften, bisweilen gibt es noch komplexere.

Temporallogik

Temporallogik erlaubt die kompakte Spezifikation von Eigenschaften von Systemabläufen.

Im Unterschied zur Aussagenlogik können auch Aussagen über den zeitlichen Ablauf gemacht werden.

Es gibt eine Reihe verschiedener Temporallogiken, z.B.

- CTL (Computation Tree Logic)
- LTL (Linear Time Logic)

In der Vorlesung wird CTL im Detail behandelt.

Temporallogik

Im Semaphorbeispiel haben wir überprüft, dass das System keinen unerwünschten Zustand erreichen kann.

In CTL kann das durch folgende Formel ausgedrückt werden.

$$\mathsf{AG}(\neg \mathit{undesired})$$

Diese Formel sagt aus, dass alle (A – all) Abläufe im Zustandsübergangssystem stets (G – generally) die Eigenschaft $\neg \mathit{undesired}$ erfüllen.

Temporallogik

Die Eigenschaft, dass stets wieder der Anfangszustand erreicht werden kann, kann in CTL wie folgt ausgedrückt werden:

$$\mathsf{AG}(\mathsf{EF}(\bigwedge_{p} q_{p\ sleep}))$$

Die Formel $\mathsf{EF}(\phi)$ besagt, dass ein Ablauf existiert (E – exists), auf dem irgendwann (F – finally) die Eigenschaft ϕ gilt.

Syntax von CTL

Die Menge der CTL-Formeln ist durch folgende Grammatik gegeben.

$$\begin{aligned}\phi, \psi ::= \; & p \mid \top \mid \bot \mid \neg\phi \mid \phi \oplus \psi \mid \mathsf{AX}\phi \mid \mathsf{EX}\phi \\ & \mid \mathsf{A}[\phi \mathsf{U} \psi] \mid \mathsf{E}[\phi \mathsf{U} \psi] \mid \mathsf{AG}\phi \mid \mathsf{AF}\phi \mid \mathsf{EG}\phi \mid \mathsf{EF}\phi\end{aligned}$$

Hier steht p für aussagenlogische Variablen und $\oplus$ steht für die zweistelligen Boole'schen Operatoren. Insbesondere ist also jede aussagenlogische Formel auch eine CTL-Formel.

Beispiel: $\mathsf{AG}(p \Rightarrow \mathsf{A}[p \mathsf{U} (\neg p \wedge \mathsf{A}[\neg p \mathsf{U} q])])$

Kein Beispiel: $\mathsf{A}[p]$ und $\phi \mathsf{U} \psi$ sind keine CTL-Formeln!

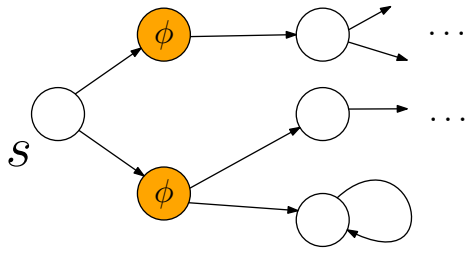
Informelle Semantik der CTL-Formeln

CTL Formeln werden relativ zu einem gegebenen Zustandsübergangssystem interpretiert.

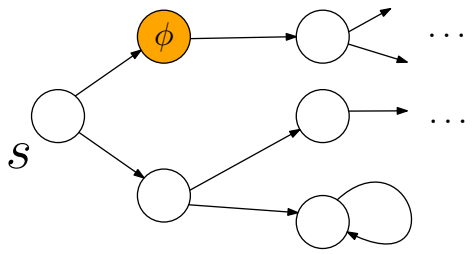
Eine CTL-Formel ϕ kann in jedem Zustand entweder gelten (= wahr sein) oder nicht.

In einem Zustand s gilt…

- …AXϕ, wenn ϕ in allen unmittelbaren Folgezuständen von s gilt.

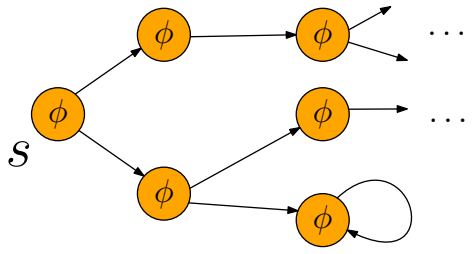


- …EXϕ, wenn ϕ in einem der unmittelbaren Folgezustände von s gilt.

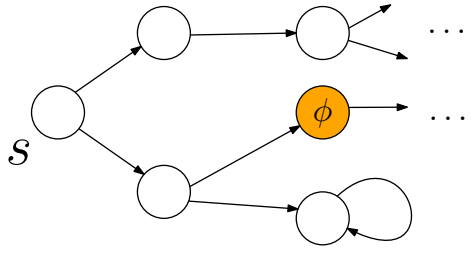


Informelle Semantik der CTL-Formeln, Forts.

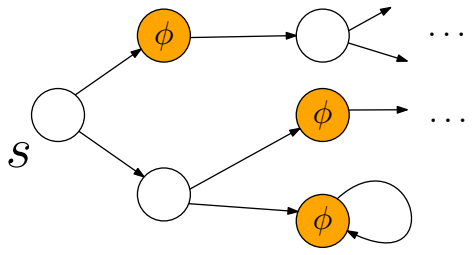
- …AGϕ, wenn ϕ auf allen von s aus erreichbaren Zuständen gilt.



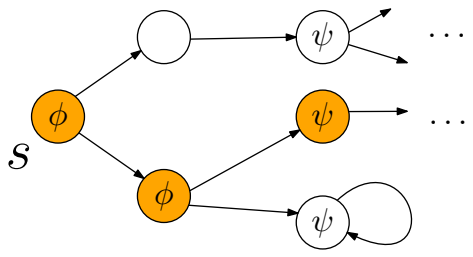
- …EFϕ, wenn man von s aus einen Zustand erreichen kann, in dem ϕ gilt.



- …AF(ϕ), wenn auf allen von s ausgehenden Ausführungspfaden irgendwann ϕ gilt.

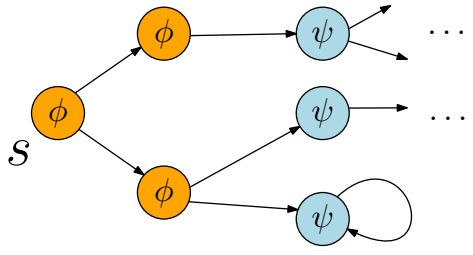


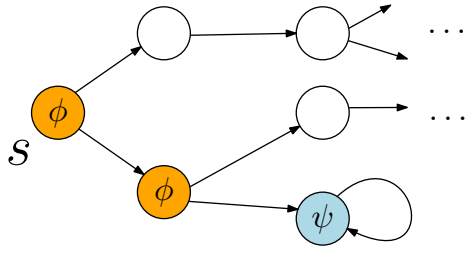
- …EG(ϕ), wenn von s aus die Ausführung so fortgesetzt werden kann, dass stets ϕ gilt.



Informelle Semantik der CTL-Formeln, Forts.

- …A$[\phi \mathrm{U} \psi]$, wenn auf allen von s ausgehenden Ausführungspfaden irgendwann ψ gilt und zumindest bis zum ersten Auftreten von ψ stets ϕ der Fall ist. (U = “until”).
- …E$[\phi \mathrm{U} \psi]$, wenn von s aus die Ausführung so fortgesetzt werden kann, dass irgendwann ψ gilt und bis dahin stets ϕ gilt.





Informelle Semantik der CTL-Formeln, Forts.

Beispiele:

- $\mathsf{AG}((\mathit{close\_door} \vee (\mathit{safe} \wedge \neg \mathit{open\_door})) \Rightarrow \mathsf{AX}\mathit{safe}) \wedge \mathsf{AG}(\mathit{heat} \Rightarrow \mathit{safe})$
- $\mathit{floor{=}2} \wedge \mathit{direction{=}up} \wedge \mathit{buttonpressed{=}5} \Rightarrow A[\mathit{direction{=}up}\ \mathsf{U}\ \mathit{floor{=}5}]$
- $\mathsf{AF}\mathit{fertig}$

Transitionssystem

Definition

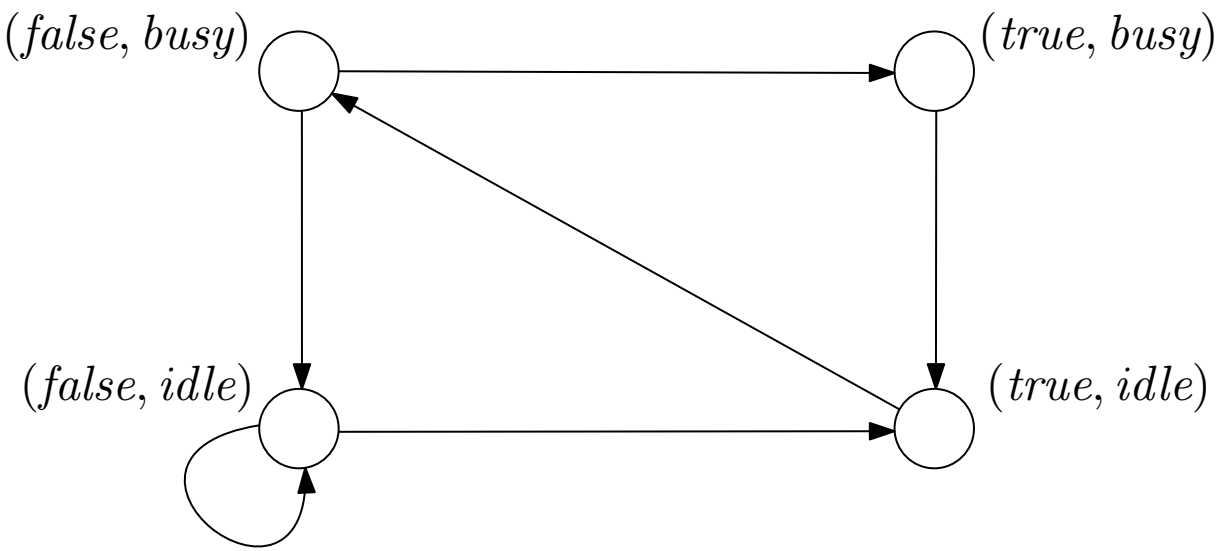
Ein *Transitionssystem* ist ein Paar $(S, \rightarrow)$, wobei

- S eine Menge von Zuständen ist, und
- $\rightarrow \subseteq S \times S$ eine binäre Relation auf S ist.
- Für jedes $s \in S$ existiert $s' \in S$ mit $s \rightarrow s'$.

- Die Menge S modelliert die Menge der globalen Zustände eines nebenläufigen Systems.
- Die Relation $\rightarrow$ heißt *Transitionsrelation*. Sie modelliert die möglichen Zustandsübergänge. Sie ergibt sich aus dem Programmtext, bzw. der Implementierung des Systems.
- Die dritte Bedingung hat technische Gründe. Liegt sie nicht bereits vor, so kann sie durch Hinzunahme eines Müllzustands s_d mit $s_d \rightarrow s_d$ künstlich hergestellt werden.

Beispiel

$$
\begin{aligned}
S &= \{(\mathit{request}, \mathit{status}) \mid \mathit{request} \in \{\mathit{true}, \mathit{false}\}, \mathit{status} \in \{\mathit{idle}, \mathit{busy}\}\} \\
\rightarrow &= \{((\mathit{false}, x), (\mathit{true}, x)) \mid x \in \{\mathit{idle}, \mathit{busy}\}\} \cup \\
&\quad \{((\mathit{true}, \mathit{idle}), (\mathit{false}, \mathit{busy}))\} \cup \\
&\quad \{((x, \mathit{busy}), (x, \mathit{idle})) \mid x \in \{\mathit{true}, \mathit{false}\}\} \cup \\
&\quad \{((\mathit{false}, \mathit{idle}), (\mathit{false}, \mathit{idle}))\}
\end{aligned}
$$



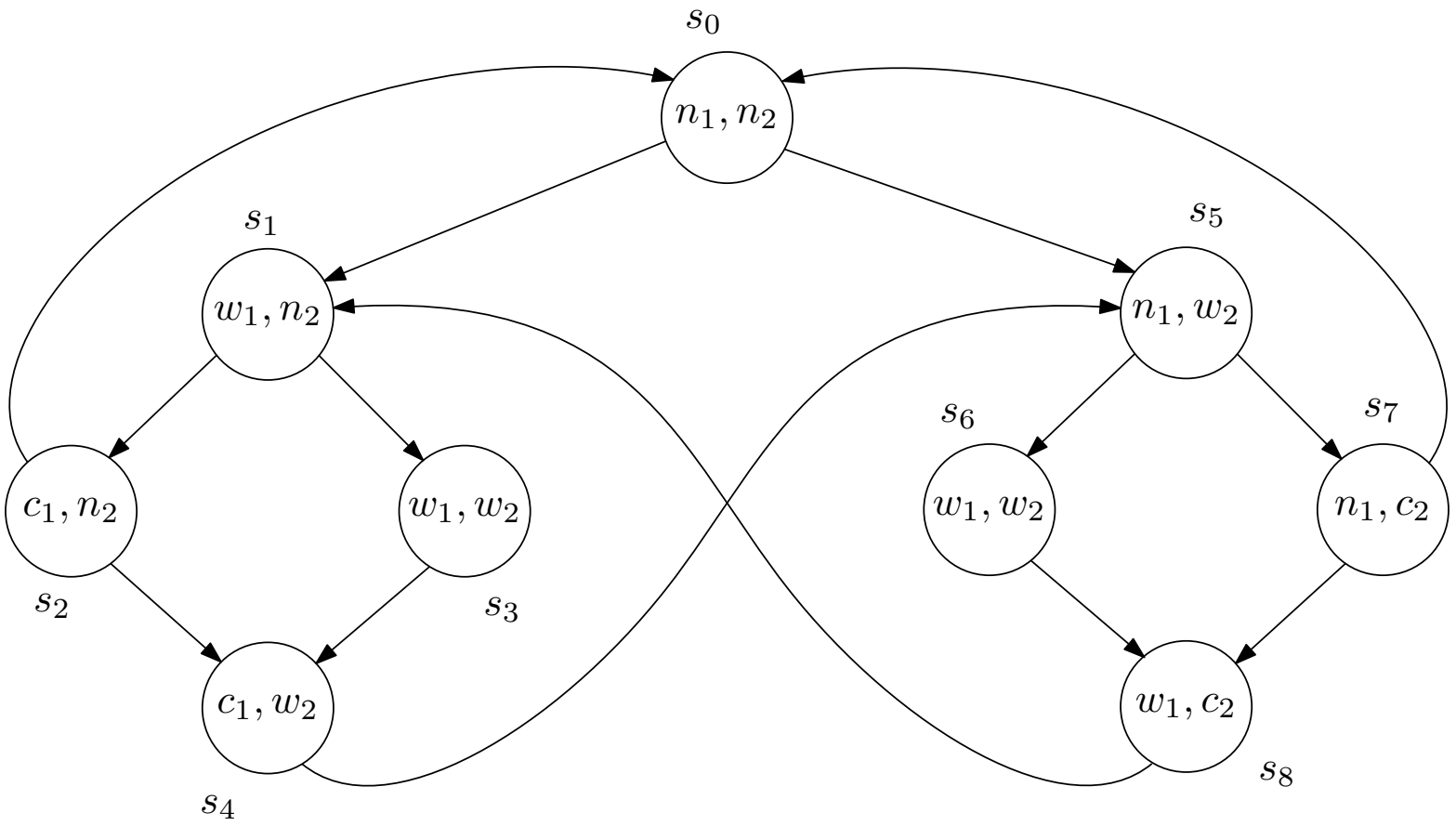
Weitere Beispiele

- Semaphor: $S = \{(\mathit{proc}_0, \mathit{proc}_1, \mathit{sem}) \mid \mathit{sem} \in \{\mathit{free}, \mathit{occ}\}, \forall i \in \{0,1\}.\mathit{proc}_i \in \{\mathit{sleep}, \mathit{wait}, \mathit{work}\}\}$
  Hier: $|S| = 18$
- Peterson:
  $S = \{(\mathit{flag}_0, \mathit{flag}_1, \mathit{turn}, \mathit{line}_0, \mathit{line}_1) \mid \forall i \in \{0,1\}.\mathit{flag}_i \in \{\mathit{true}, \mathit{false}\} \;\&\; \mathit{turn} \in \{0,1\} \;\&\; \mathit{line}_i \in \{0,1,2,3,4\}\}$
  Hier: $|S| = 2^2 \cdot 2 \cdot 5^2 = 200$
- Bauer, Hund, Katze, Maus: $S = \{(\mathit{pos}_B, \mathit{pos}_H, \mathit{pos}_K, \mathit{pos}_M) \mid \forall x \in \{B, H, K, M\}.\, \mathit{pos}_x \in \{\mathit{links}, \mathit{rechts}\}\}$
  Hier: $|S| = 2^4 = 16$.

NB: Die Transitionsrelation $\rightarrow$ ist hier jeweils weggelassen.

Weitere Beispiele

Der von Zustand $s_0 = (\mathit{sleep}, \mathit{sleep}, \mathit{free})$ aus erreichbare Teil des Semaphor-Transitionssystems:



Formale Semantik von CTL

Die Semantik von CTL-Formeln wird bezüglich einer Interpretation festgelegt.

Definition

Eine *Interpretation* $\mathcal{I}$ besteht aus einem endlichen Transitionssystem $\mathit{Tr}(\mathcal{I}) = (S, \rightarrow)$ sowie einer Menge von Zuständen $\mathcal{I}(p) \subseteq S$ für jede aussagenlogische Variable p.

Sei $\mathcal{I}$ eine Interpretation $\mathcal{I}$ mit $\mathit{Tr}(\mathcal{I}) = (S, \rightarrow)$.

Die CTL-Semantik legt für jede Formel ϕ und jeden Zustand $s \in S$ fest, ob die Formel in diesem Zustand bezüglich der Interpretation $\mathcal{I}$ gilt.

Wir schreiben kurz $s \models_{\mathcal{I}} \phi$ für "ϕ gilt im Zustand s (bezüglich $\mathcal{I}$)" und definieren diesen Begriff auf den nächsten Folien.

Definition der Semantik

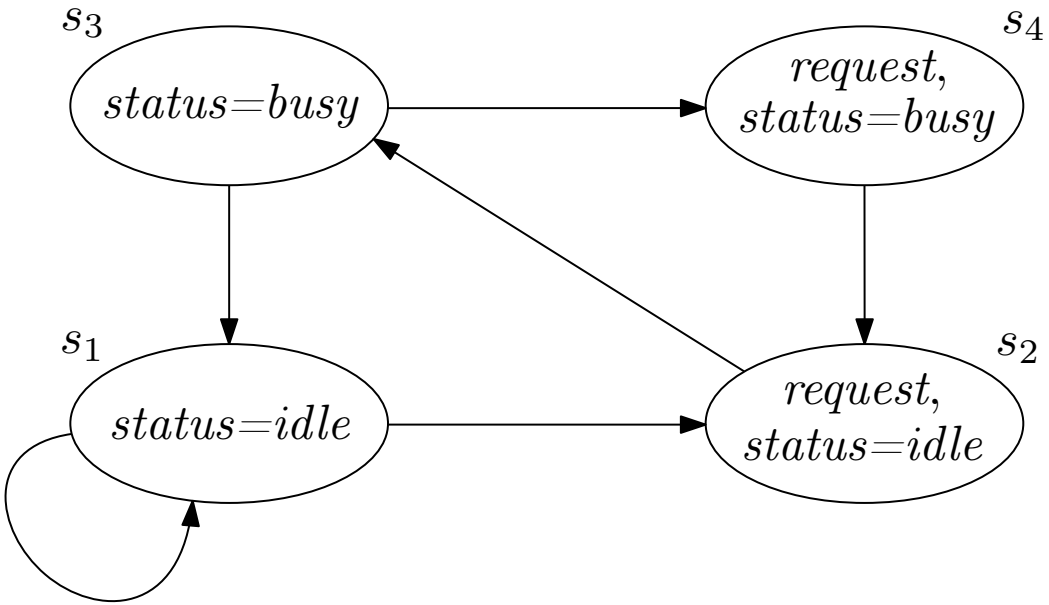
- $s \models_{\mathcal{I}} p$ genau dann wenn $s \in \mathcal{I}(p)$.
- $s \models_{\mathcal{I}} \neg\phi$ genau dann wenn $s \models_{\mathcal{I}} \phi$ nicht gilt (auch geschrieben als $s \not\models_{\mathcal{I}} \phi$).
- $s \models_{\mathcal{I}} \phi \wedge \psi$ genau dann wenn $s \models_{\mathcal{I}} \phi$ und $s \models_{\mathcal{I}} \psi$.
- die anderen Boole'schen Operatoren $\vee$, $\Rightarrow$, etc. sind analog.
- $s \models_{\mathcal{I}} \mathrm{EX}\phi$ genau dann wenn $s' \in S$ existiert mit $s \rightarrow s'$ und $s' \models_{\mathcal{I}} \phi$.
- $s \models_{\mathcal{I}} \mathrm{AX}\phi$ genau dann wenn für alle $s' \in S$ mit $s \rightarrow s'$ gilt: $s' \models_{\mathcal{I}} \phi$.

Definition der Semantik, Fortsetzung

- $s \models_{\mathcal{I}} \mathsf{AG}\phi$ gdw: Alle unendlichen Pfade $s = s_0 \to s_1 \to s_2 \to s_3 \to \ldots$ haben die Eigenschaft, dass $s_i \models_{\mathcal{I}} \phi$ für alle $i \geqslant 0$ gilt.
- $s \models_{\mathcal{I}} \mathsf{EG}\phi$ gdw: Es gibt einen unendlichen Pfad $s = s_0 \to s_1 \to s_2 \to s_3 \to \ldots$ mit der Eigenschaft, dass $s_i \models_{\mathcal{I}} \phi$ für alle $i \geqslant 0$ gilt.
- $s \models_{\mathcal{I}} \mathsf{EF}\phi$ gdw: Es gibt einen unendlichen Pfad $s = s_0 \to s_1 \to s_2 \to s_3 \to \ldots$ mit der Eigenschaft, dass $s_i \models_{\mathcal{I}} \phi$ für ein $i \geqslant 0$ gilt.
- $s \models_{\mathcal{I}} \mathsf{AF}\phi$ gdw: Alle unendlichen Pfade $s = s_0 \to s_1 \to s_2 \to s_3 \to \ldots$ haben die Eigenschaft, dass $s_i \models_{\mathcal{I}} \phi$ für ein $i \geqslant 0$ gilt.

Beispiel

Die Interpretation $\mathcal{I}$ mit dem Transitionssystem von Folie 120 sowie $\mathcal{I}(\mathit{request}) = \{s_2, s_4\}, \mathcal{I}(\mathit{status{=}idle}) = \{s_1, s_2\}$ und $\mathcal{I}(\mathit{status{=}busy}) = \{s_2, s_3\}$ wird folgendermaßen dargestellt.



Es gilt:

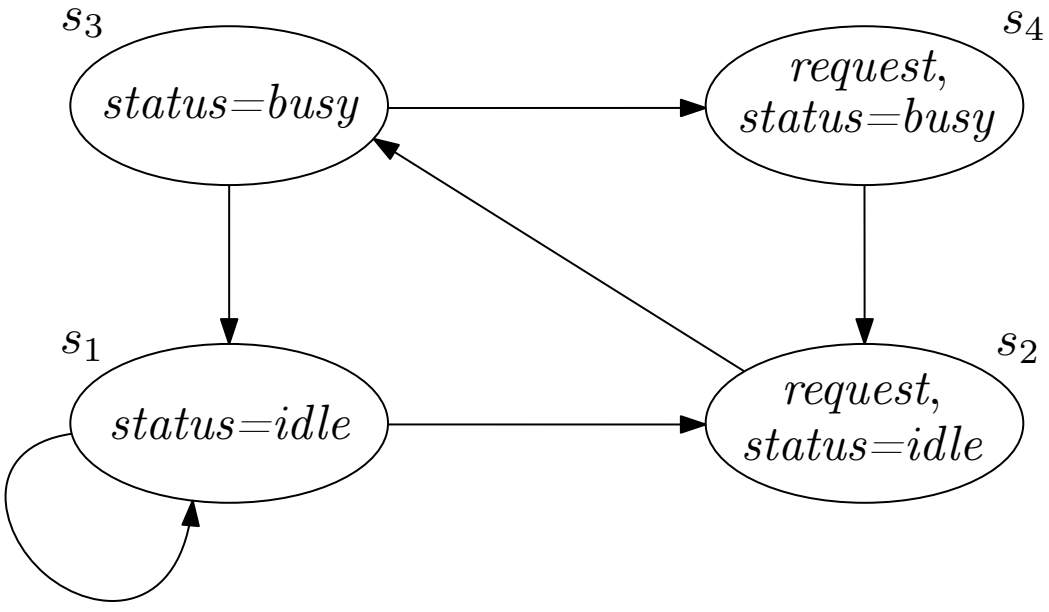
$s_1 \models_{\mathcal{I}} \mathsf{AF}\neg \mathit{request}$ $\quad$ $s_1 \models_{\mathcal{I}} \mathsf{AG}(\mathit{request} \Rightarrow \mathsf{EF}(\mathit{status{=}busy}))$

$s_1 \models_{\mathcal{I}} \mathsf{EG}\neg \mathit{request}$ $\quad$ $s_1 \models_{\mathcal{I}} \mathsf{AG}(\neg\mathsf{EG}(\mathit{status{=}busy}))$

Semantik der Until-Formeln

- $s \models_{\mathcal{I}} \mathsf{E}[\phi \mathsf{U} \psi]$ gdw: Es gibt einen Pfad $s = s_0 \to s_1 \to s_2 \to s_3 \to \ldots s_n$ mit der Eigenschaft, dass dass $s_n \models_{\mathcal{I}} \psi$ gilt sowie dass $s_i \models_{\mathcal{I}} \phi$. für alle $i < n$ gilt.
- $s \models_{\mathcal{I}} \mathsf{A}[\phi \mathsf{U} \psi]$ gdw: Alle unendlichen Pfade $s = s_0 \to s_1 \to s_2 \to s_3 \to \ldots$ haben die Eigenschaft, dass ein $n \geqslant 0$ existiert mit $s_n \models_{\mathcal{I}} \psi$ und $s_i \models_{\mathcal{I}} \phi$ für alle $i < n$.

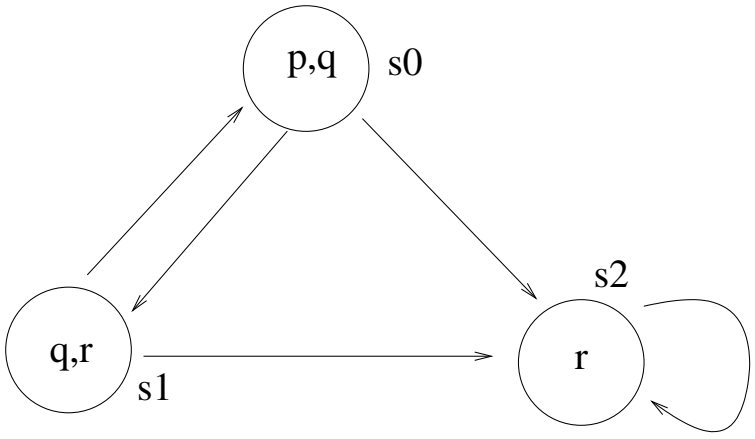
Beispiel



Es gilt:

$$s_1 \models_{\mathcal{I}} \mathsf{AG}(request \Rightarrow \mathsf{A}[request\ \mathsf{U}\ status{=}busy])$$

Beispiel



$s_0 \models_{\mathcal{I}} p \wedge q$

$s_0 \models_{\mathcal{I}} \top$

$s_0 \models_{\mathcal{I}} \neg \mathsf{AX}(q \wedge r)$

$s_1 \models_{\mathcal{I}} \mathsf{EG} r$

$s_0 \models_{\mathcal{I}} \mathsf{AF} r$

$s_0 \models_{\mathcal{I}} \mathsf{A}[p \mathsf{U} r]$

$s_0 \models_{\mathcal{I}} p \wedge \neg r$

$s_0 \models_{\mathcal{I}} \mathsf{EX}(q \wedge r)$

$s_0 \models_{\mathcal{I}} \neg \mathsf{EF}(p \wedge r)$

$s_2 \models_{\mathcal{I}} \mathsf{AG} r$

$s_0 \models_{\mathcal{I}} \mathsf{E}[(p \wedge q) \mathsf{U} r]$

Äquivalenzen

Äquivalenz von CTL-Formeln

Zwei CTL-Formeln ϕ und ψ sind *äquivalent*, geschrieben $\phi \iff \psi$, wenn für alle Interpretationen $\mathcal{I}$ und alle Zustände s gilt: $s \models_{\mathcal{I}} \phi$ gdw. $s \models_{\mathcal{I}} \psi$.

Sind $\phi \iff \psi$ aussagenlogisch äquivalente Formeln, so auch als CTL-Formeln. Z.B.: $\mathsf{AG}(p) \vee \mathsf{AG}(p) \iff \mathsf{AG}(p)$.

Wichtige Äquivalenzen:

$$\neg\mathsf{AG}(\phi) \iff \mathsf{EF}(\neg\phi) \qquad \neg\mathsf{AF}(\phi) \iff \mathsf{EG}(\neg\phi)$$

$$\neg\mathsf{EF}(\phi) \iff \mathsf{AG}(\neg\phi) \qquad \neg\mathsf{EG}(\phi) \iff \mathsf{AF}(\neg\phi)$$

$$\mathsf{AF}(\phi) \iff \mathsf{A}[\top\mathsf{U}\phi] \qquad \mathsf{EF}(\phi) \iff \mathsf{E}[\top\mathsf{U}\phi]$$

$$\mathsf{A}[\phi\mathsf{U}\psi] \iff \neg(\mathsf{E}[\neg\psi\mathsf{U}(\neg\phi \wedge \neg\psi)] \vee \mathsf{EG}(\neg\psi))$$

Äquivalenzen

Satz

Für jede CTL-Formel ϕ gibt es eine äquivalente Formel, in der neben Variablen nur die Operatoren $\neg$, $\wedge$, $\bot$, EX, AF, E$[-\mathsf{U}-]$ verwendet werden.

Beweis: Übung