



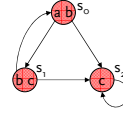
KRIPKE, BERECHNUNGSBAUM UND TEMPORALE LOGIK

Seminar "Model-Checking" WSo8/09

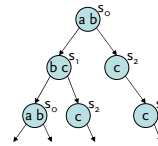
Daniela Weinberg
weinberg@informatik.hu-berlin.de

ZUSTANDSGRAPH UND BERECHNUNGSBAUM

- Transitionssystem (Kripke Struktur)
 - Eigenschaften: a, b, c



- unendlicher Berechnungsbaum ausgehend von s_0



KORREKTHEITSEIGENSCHAFTEN

- Sicherheit
 - "nichts schlechtes passiert"
 - jeder endliche Präfix erfüllt bestimmte Eigenschaften
- Lebendigkeit
 - "etwas Gutes passiert"
 - es bleibt immer möglich, dass das Gute in Zukunft passiert



TEMPORALE LOGIK

Seminar "Model-Checking" WSo8/09

Daniela Weinberg
weinberg@informatik.hu-berlin.de

MODEL CHECKING

- Abstraktion des physischen Systems
 - Modell M
- nachzuweisende formale Eigenschaften des Systems
 - Formel ϕ
- Frage – gilt ϕ in M?

$$M \models \phi$$

DIE FORMEL ϕ

- wollen interessante Eigenschaften von Systemen beschreiben
 - "Wenn die Ampel auf rot steht, wird sie irgendwann auf grün wechseln."
 - "Die Ampel wird nie zugleich auf rot und grün stehen."
 - also: Aussagenlogik nicht ausreichend

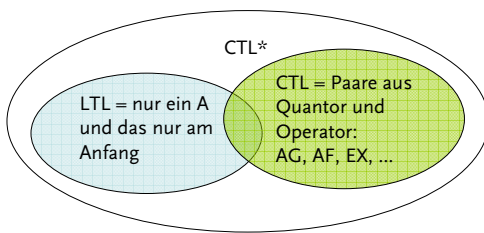
TEMPORALE LOGIK – CTL*

- **Computational Tree Logic**
 - Fundament: Aussagenlogik
 - formales System, das beschreibt wie sich der Wahrheitswert von Aussagen über die Zeit verändert
 - für nichtterminierende, nebenläufige Systeme z.B. Betriebssysteme, Kommunikationsprotokolle

DEFINITION VON CTL*

- Zustandsaussagen
- Boolesche Verknüpfungen
- Pfadquantoren:
 - E – entlang mindestens eines Pfades („there exists one path“)
 - A – entlang aller Pfade („along all paths“)
- Temporale Operatoren:
 - X – unmittelbar folgender Zustand („next state“)
 - F – ein irgendwann folgender Zustand („some future state“); Zukunft beinhaltet Gegenwart
 - G – alle folgenden Zustände („globally“)
 - U – ϕ gilt ununterbrochen bis ψ eintritt („until“)

CTL* FRAGMENTE



CHRONOLOGIE DER TEMPORALEN LOGIKEN

- LTL - Linear-time Temporal Logic (~1960)
 - lineares Zeitmodell
 - Aussagen gelten immer für alle Pfade
- CTL - Computation Tree Logic (~1980)
 - Zeit als Baum: Verzweigung in unterschiedliche Versionen der Zukunft (Pfade)
 - Aussagen können auf bestimmte Pfade beschränkt werden
- CTL* (1986)
 - Erweiterung der Ausdrucksmöglichkeiten von CTL und LTL
 - Zeit als Baum
 - freie Verschachtelung der Temporaloperatoren

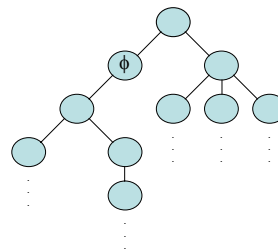
SYNTAX

- induktive Definition von CTL-Formeln:

$$\phi ::= \top \mid \perp \mid p \mid (\neg\phi) \mid (\phi \wedge \psi) \mid (\phi \vee \psi) \mid (\phi \rightarrow \psi) \mid AX\phi \mid EX\phi \mid AF\phi \mid EF\phi \mid AG\phi \mid EG\phi \mid A[\phi U \psi] \mid E[\phi U \psi]$$
- mit p aus der Menge der atomaren Aussagen

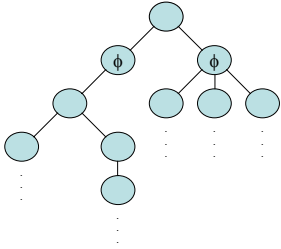
SEMANTIK - EX ϕ

- System, dessen Startzustand EX ϕ erfüllt



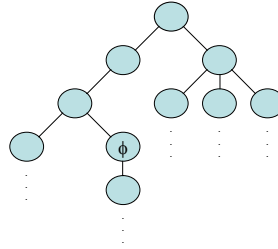
SEMANTIK - AX ϕ

- System, dessen Startzustand AX ϕ erfüllt



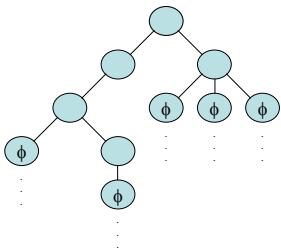
SEMANTIK - EF ϕ

- System, dessen Startzustand EF ϕ erfüllt



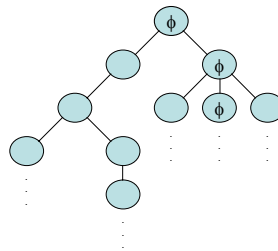
SEMANTIK - AF ϕ

- System, dessen Startzustand AF ϕ erfüllt



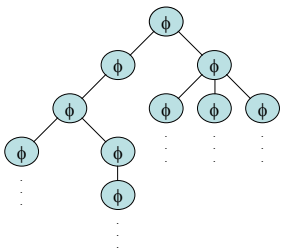
SEMANTIK - EG ϕ

- System, dessen Startzustand EG ϕ erfüllt



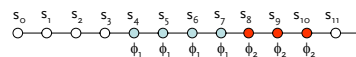
SEMANTIK - AG ϕ

- System, dessen Startzustand AG ϕ erfüllt



SEMANTIK - $\phi_1 U \phi_2$

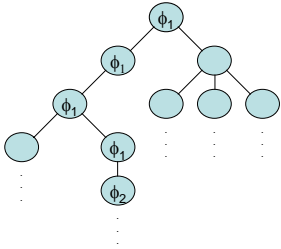
- entlang eines Pfades muß ϕ_1 stetig bis zum nächsten Vorkommen von ϕ_2 erfüllt sein



- formal: $M \models \phi_1 U \phi_2$
gdw. $\exists j \geq 0 : (M, s_j \models \phi_2 \wedge (\forall 0 \leq k < j : M, s_k \models \phi_1))$

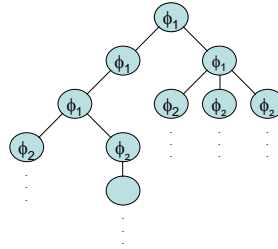
SEMANTIK – $E[\phi_1 \cup \phi_2]$

- System, dessen Startzustand $E[\phi_1 \cup \phi_2]$ erfüllt



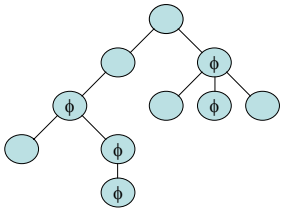
SEMANTIK – $A[\phi_1 \cup \phi_2]$

- System, dessen Startzustand $A[\phi_1 \cup \phi_2]$ erfüllt



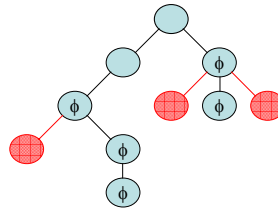
SEMANTIK – $AF EG \phi$

- $M, s_1 \models AF \phi$ gdw., für alle Pfade $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \dots$ gibt es ein s_i , so dass $M, s_i \models \phi$
- $M, s_1 \models EG \phi$ gdw., es gibt einen Pfad $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \dots$, so dass für alle s_i gilt $M, s_i \models \phi$



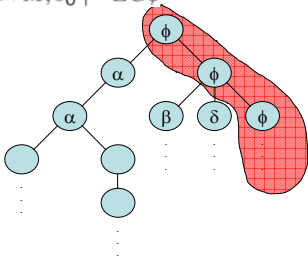
SEMANTIK – $AF AG \phi$

- $M, s_1 \models AF \phi$ gdw., für alle Pfade $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \dots$ gibt es ein s_i , so dass $M, s_i \models \phi$
- $M, s_1 \models AG \phi$ gdw., für alle Pfade $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \dots$ gilt für alle s_i $M, s_i \models \phi$



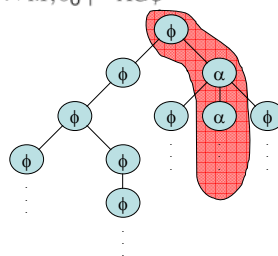
ZEUGEN UND GEGENBEISPIELE I

- wann gilt eine Eigenschaft?
 - für jede E-Formel gibt es einen Zeugenpfad
 - Beispiel: $M, s_0 \models EG \phi$



ZEUGEN UND GEGENBEISPIELE II

- wann gilt eine Eigenschaft?
 - für jede A-Formel gibt es einen Gegenbeispielpfad
 - Beispiel: $M, s_0 \models AG \phi$



KLEINE ÜBUNG

- Seien die Aussagen P und Q gegeben:
 - P: "Ich mag Schokolade."
 - Q: "Es ist warm draußen."
- AG P**
 - Ab sofort mag ich Schokolade, egal was passiert.
- EF P**
 - Es ist möglich, dass ich eines Tages Schokolade mag – und das wenigstens für einen Tag
- AF EG P**
 - Es ist immer möglich, dass ich plötzlich anfange Schokolade für den Rest der Zeit zu mögen. (Achtung: Rest des Lebens wäre endlich, **G** ist aber unendlich)

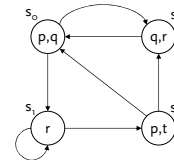
KLEINE ÜBUNG (FORTSETZUNG)

- A(PUQ)**
 - Ich werde von jetzt an Schokolade mögen bis es draußen warm ist. Ist es einmal warm, weiß ich nicht, ob ich dann noch jemals Schokolade mag. Es ist also ganz sicher, dass es einmal warm wird – auch wenn es nur für einen Tag ist.

LTL ODER CTL

- GF P**
 - LTL aber nicht CTL
- AG(P ⇒ ((EX Q) ∨ (EX Q)))**
 - CTL aber nicht LTL

ÜBUNG



- gegeben ist System M; {p,q,r,t} seien atomare Aussagen
- ausgehend von s₀, zeichne den Berechnungsbaum bis zu einer Tiefe von 4.
- überprüfe, ob $M, s_0 \models \phi$ gilt, mit
 - $\phi = \text{AF } t$
 - $\phi = \text{AG } (\text{EF } (p \vee r))$
 - $\phi = \text{E } (t \text{ U } q)$
 - $\phi = \text{EG } r$