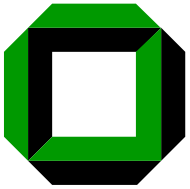
Formale Systeme

Prof. Dr. Bernhard Beckert

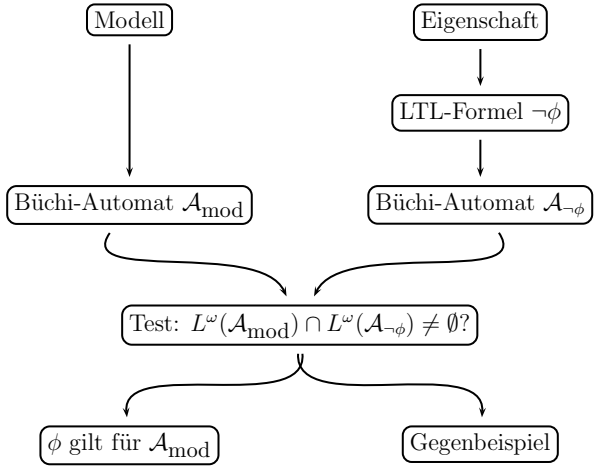
Fakultät für Informatik
Universität Karlsruhe (TH)



Winter 2008/2009

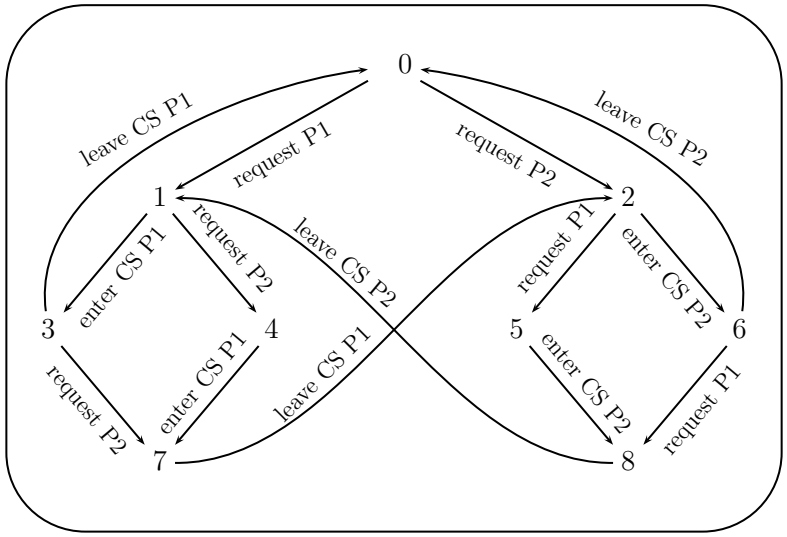
Modellprüfung für LTL

Übersicht



Exklusive Zugriffskontrolle

Ereignisbasiertes Automatenmodell



Aussagenlogische Signatur Σ

Für $i \in \{1, 2\}$:

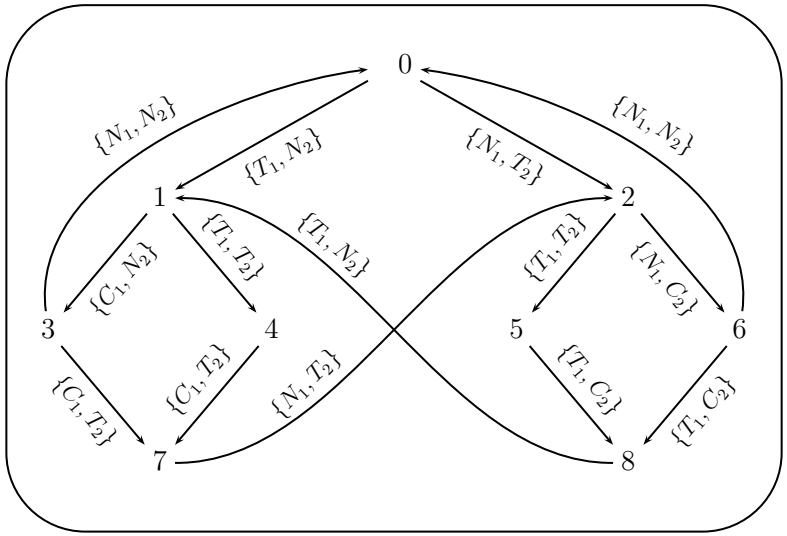
N_i	Prozeß i befindet sich in einer nichtkritischen Region
T_i	Prozeß i befindet sich in der Anmeldephase
C_i	Prozeß i befindet sich in einer kritischen Region

Automatenvokabular $V = 2^\Sigma$.

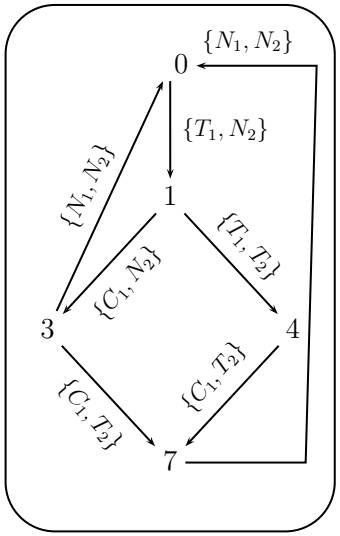
Ersetze die Ereignismarkierung einer Kante durch die Menge der Atome aus Σ, die im Zielzustand wahr werden.

Exklusive Zugriffskontrolle

Aussagenbasiertes Automatenmodell



Reduzierter Automat $\mathcal{A}_{me}$



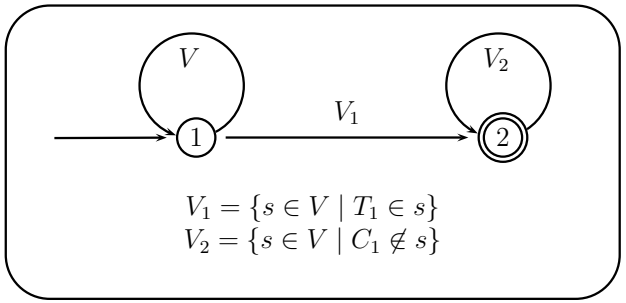
Zu verifizierende Eigenschaft

Wenn Prozeß 1 sich zur exklusiven Nutzung der Ressource anmeldet, dann wird er schließlich auch den Zugang erhalten.

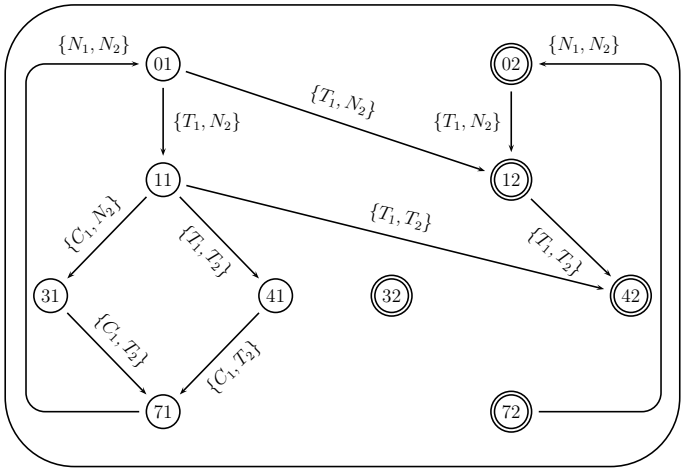
Als LTL-Formel: $\Box(T_1 \rightarrow \Diamond C_1)$

Negierte Formel: $\Diamond(T_1 \wedge \Box\neg C_1)$

Büchi-Automat $\mathcal{B}_{em}$ dazu:



Produktautomat $\mathcal{A}_{me} \times \mathcal{B}_{me}$



Offensichtlich gilt: $L^{\omega}(\mathcal{A}_{me} \times \mathcal{B}_{me}) = \emptyset$