

# 23. Behavioral Model Checking (Prüfung von Verhaltensmodellen)

1

- 1) Modellprüfung – Überblick
- 2) Realzeit-Modellprüfung

Prof. Dr. U. Alsmann

Technische Universität Dresden

Institut für Software- und  
Multimediatechnik

<http://st.inf.tu-dresden.de>

Version 13-1.0, 05.12.13



Softwareentwicklungswerkzeuge (SEW) © Prof. Uwe Alsmann

## Obligatory Literature

- 2
  - ▶ Markus Müller-Olm, David Schmidt, Bernhard Steffen. Model-Checking. A Tutorial Introduction. Springer LNCS, Volume 1694, 1999, p 848ff
    - <http://www.springerlink.com/content/1437dulbgk67j6m/>
  - [BW04] Timed Automata: Semantics, Algorithms and Tools, Johan Bengtsson and Wang Yi. In Lecture Notes on Concurrency and Petri Nets. W. Reisig and G. Rozenberg (eds.), LNCS 3098, Springer-Verlag, 2004
    - <http://www.it.uu.se/research/group/darts/papers/texts/by-lncs04.ps>
  - [BDL04] A Tutorial on Uppaal, Gerd Behrmann, Alexandre David, and Kim G. Larsen. In proceedings of the 4th International School on Formal Methods for the Design of Computer, Communication, and Software Systems (SFM-RT'04). LNCS 3185.
    - <http://www.cs.auc.dk/~adavid/publications/21-tutorial.pdf>



## Other Literature

3

- ▶ E. Clarke's course on Model Checking <http://www.cs.cmu.edu/~emc/15817-s05/>
- ▶ E. Clarke. Model Checking. Springer LNCS 1346, 1997  
<http://www.springerlink.com/index/v1h70v370p172844.pdf>
- ▶ E. M. Clarke, E. A. Emerson, A. P. Sistla. Automatic Verification of Finite-State Concurrent Systems Using Temporal Logic Specifications, ACM Transactions on Programming Languages and Systems, vol 8, number 2, pages 244—263, apr 1986,
  - An early version appeared in Proc. 10th ACM Symposium on Principles of Programming Languages, 1983
  - <http://www.acm.org/pubs/toc/Abstracts/0164-0925/5399.html>

Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)



## 23.1 Model Checking – An Overview

4



# Problem

5

- ▶ Wie kann man statisch, vor Laufen des Systems, Aussagen über sein Verhalten machen?
- ▶ Antwort: mit abstrakter Interpretation, die allerdings verschieden realisiert sein kann:
- ▶ Lösung 1: Durch Programmanalyse mit abstrakter Interpretation
  - Spezifiziere das System, seine operationale Semantik als Zustandssystem
  - Interpretiere abstrakt und gewinne konservative Abschätzungen wie Typprüfungen und Konformität zu Metamodellen
  - Ansätze wie AG, RAG, abstrakte Interpretationsgeneratoren wie PAG
  - Verifikationen auf der Basis der denotationellen oder axiomatischen Semantik
- ▶ Lösung 2: Spezifiziere das System, seine operationale Semantik als Zustandssystem, in Logik
  - Lasse eine Deduktionsmaschine (reasoner) laufen, um die Analyse zu machen
  - Die abstrakte Interpretation wird also durch die Dekuktionsmaschine durchgeführt
  - **Modellprüfer (model checker)** sind solche speziellen Deduktionsmaschinen, die einen endlichen Automaten interpretieren, um die Gültigkeit von Prädikaten nachzuweisen.
- ▶ Lösung 3: mit dem Graph-Logik-Isomorphismus:
  - Spezifikation des Zustandssystems als endlicher Graph (statt mit Logik)
  - Dann ergibt sich der dynamische Zustandsraum als unendlicher Baum von Zuständen
  - Auswertung von Logik-Formeln durch "Weiterhangeln" im Zustandsraum
  - Abstrakte Interpretation durch Graphanalyse und Graphtransformation

Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)



# Behavioral Model Checking (Prüfung des Semantischen Modells)

6

- ▶ Model checking führt eine Interpretation eines entscheidbaren Programms durch, konkret oder abstrakt, um die Gültigkeit eines Prädikats in einem Zustand zu beweisen
  - "is the predicate a semantic model of the program"?
- ▶ Voraussetzung: Modellierung eines Programms als reguläres Zustandssystems oder endlicher Zustandsgraph
  - z. B. mit endlichen Automaten oder Petri-Netzen oder domänenspezifischen Sprachen, die darauf übersetzen (Statecharts, Entscheidungstabellen, etc.)
    - auch nebenläufige Systeme
  - Beschreiben von Anforderungen an das System und an seine Zustände mit Logik
    - z. B. mit temporaler Logik (Pfadbasierter Logik)
  - Im Folgenden Beschränkung auf automatenbasierte Programme, d.h. entscheidbare Programme
- ▶ Verifikation der Anforderungen dann möglich:
  - durch Berechnung aller möglichen Zustände des Systems sowie aller in diesen gültigen Prädikate
  - Man führt also eine Interpretation des entscheidbaren Programms durch
  - Achtung: weil das Programm entscheidbar ist, muss nicht *abstrakt interpretiert* werden, sondern es kann konkret interpretiert werden

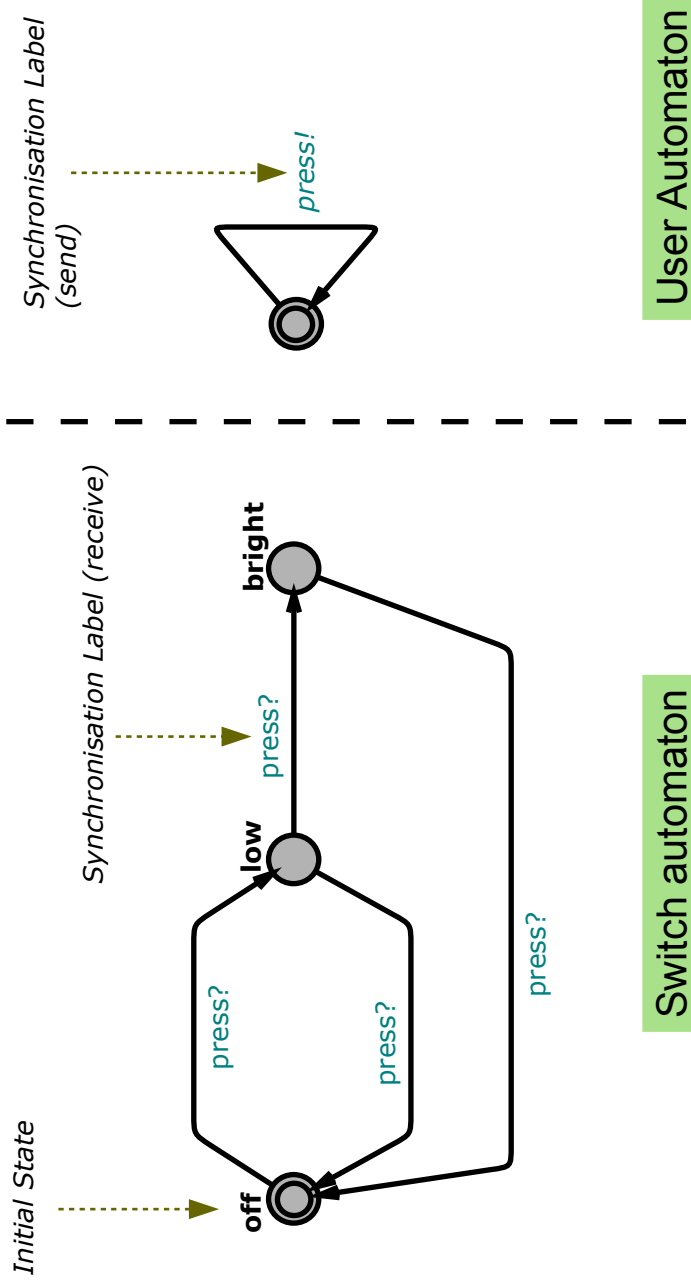
Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)



# Communicating Automata for a Double-Click Switch (Doppelklick-Lichtschalter)

7

- Can we prove something about this system of two automata?



Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)

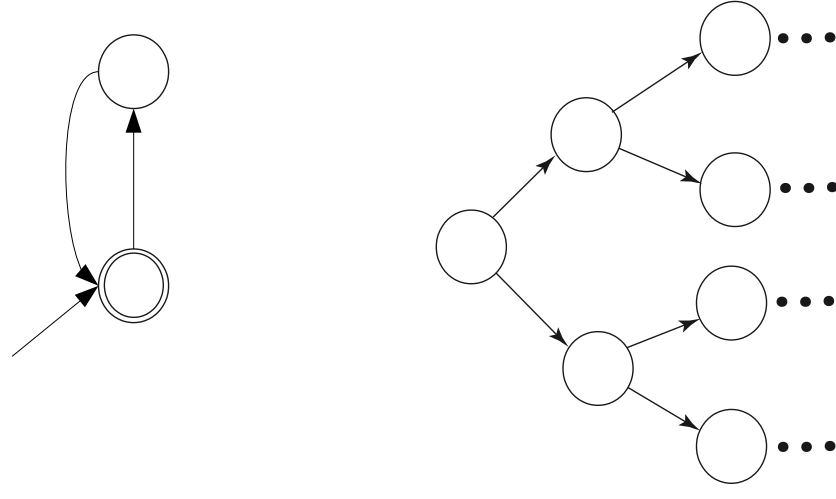


## Interpretation eines Automaten mit Model-Checking

8

- Schritt 1: Komposition aller kommunizierenden Automaten zum **Systemautomat**
  - Endliche Automaten können komponiert werden (Produkt), die Ergebnisse können aber exponentiell größer sein!
- Schritt 2: Vom Gesamtsystem (Systemautomat) wird **Berechnungsbaum** (oder Zustandsraum, **reachability tree**) erstellt
  - Der Berechnungsbaum ergibt sich durch Interpretation der Automaten
  - Er enthält alle möglichen Zustände des Systems
  - Wurzel ist der eindeutige Startzustand des Systems
  - Er ist zwar unendlich groß/tief/breit, enthält aber nur regulär viele Pfade (da von einem endlichen Automaten stammend)
- Schritt 3: **Anfragen** an den Berechnungsbaum (Queries): Für welche erreichbaren Zustände gilt welches Prädikat?

Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)



# Operators of Computational Tree Logic (CTL)

- ▶ CTL uses propositional logic about states, path quantifiers and temporal quantifiers (aussagenlogische Formeln über Zuständen, Pfadquantoren und Temporalquantoren)
- ▶ Let be  $\varphi, \psi$  propositional formulas in the following

- Examples:
  - $x > 1$
  - $(P1.attribute3 == true \text{ and } (P2.i == 5)) \text{ or } (clock > 200)$
  - not deadlock

- ▶ **Path Quantifiers (Pfadquantoren):** on which path starting from a state holds a formula?

- **A** auf allen Pfaden (all paths)
- **E** auf mindestens einem Pfad (some paths)

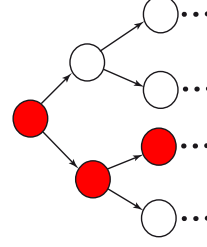
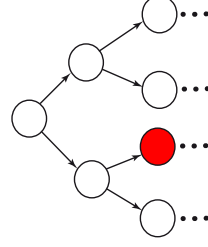
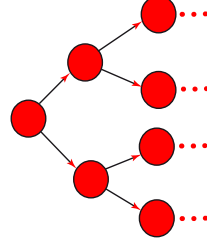
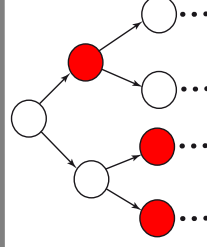
- ▶ **Temporal quantifiers:** When does the formula hold?

- **F** **somewhen** along the path (*future, finally*)
- **G** in all states along the path (*globally*)

# Operators (2)

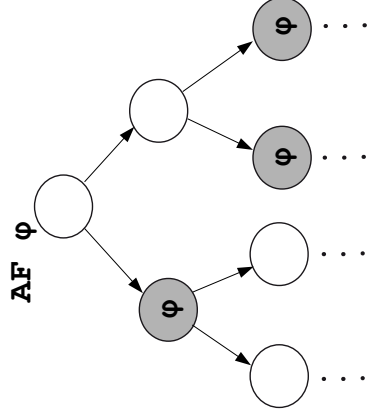
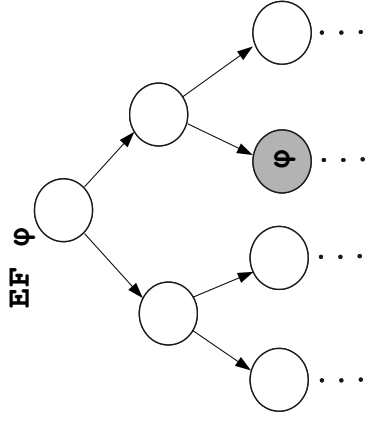
- ▶ Pfad-Temporalquantor-Operatoren über Zustandsformeln:

- **AF**  $\varphi$  auf allen Pfaden  
irgendwann gilt einmal (all-exists: on all paths exists)
- **AG**  $\varphi$  auf allen Pfaden in allen erreichbaren Zuständen (all-globally: on all paths in all states)
- **EF**  $\varphi$  irgendwo entlang eines Pfades irgendwann (exists-finally; future: on a path finally exists)
- **EG**  $\varphi$  irgendwo in einem Pfad in allen Zuständen entlang des Pfades (exists-globally)



# Example Queries on the Computation Tree (Berechnungsbaum)

11

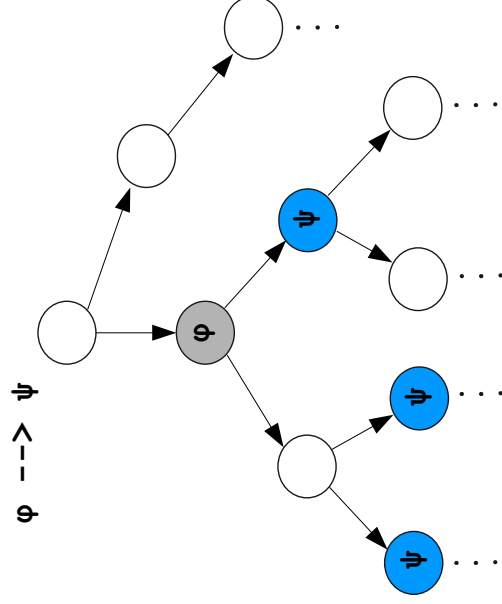


# Complex Operators (2)

12

► Leads-To Operator  $\varphi \dashrightarrow \psi$

– If  $\varphi$  holds in a state, then *some*when in the future holds  $\psi$



## Example Queries for the Double-Click Light Switch

13

- ▶ **EF** (Switch.bright)
  - State *bright* can be reached
  - is satisfied
- ▶ **AG** (not deadlock)
  - Every state in the state space has a successor
  - is satisfied
- ▶ Switch.low  $\rightarrow$  (Switch.off || Switch.bright)
  - If Switch.low is reached, then on every path holds somewhere formula (Switch.off || Switch.bright)
  - State *low* will be left
  - $\Rightarrow$  is not satisfied because User does not always click, so that *low* can be left

Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)



## 23.2. Realzeit-Modellprüfung (Real-Time Model Checking)

14

.. mit UPPAAL..

Achtung: Folien mit 23.1, Standard-Model-Checking, vergleichen, um die Unterschiede zu sehen



# Real-time Model-Checking

15

- ▶ Modellierung eines Systems in formaler, entscheidbarer Sprache
  - z. B. Automaten, Petri-Netze
- ▶ Hier: Beschreiben von Anforderungen an das System mit temporaler Logik, erweitert mit **Bedingungen über “real-time variables” (Realzeitbedingungen, Realzeitaspekt)**
- ▶ Verifikation der Anforderungen möglich:
  - durch Berechnung aller möglichen Zustände des Systems **und Überprüfung der Realzeitbedingungen**

Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)



# UPPAAL

<http://www.uppaal.org/>

16

- ▶ Model-Checking-Tool für Echtzeitsysteme
  - Verifikationseengine in C++
- ▶ graphische Benutzeroberfläche in Java
- ▶ Anforderungen werden mittels einer Untermenge von CTL (computation tree logic) formuliert
- ▶ UPPAAL – Modellierungssprache:
  - parallel laufende erweiterte **Timed Automata (TA)**: Endliche Automaten mit Uhren
  - Uhren haben als Wertebereich reelle Zahlen
  - alle Uhren schalten synchron
  - Uhren können zurückgesetzt werden
- ▶ Systemzustand: Zustand aller TA, Uhren, Variablen
- ▶ Erweiterungen:
  - diskrete Variablen (int, boolean; strukturierte Datentypen, Arrays)
  - Konstanten
  - C-ähnliche Funktionen
  - Synchronisation der Automaten über *Channels*

Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)

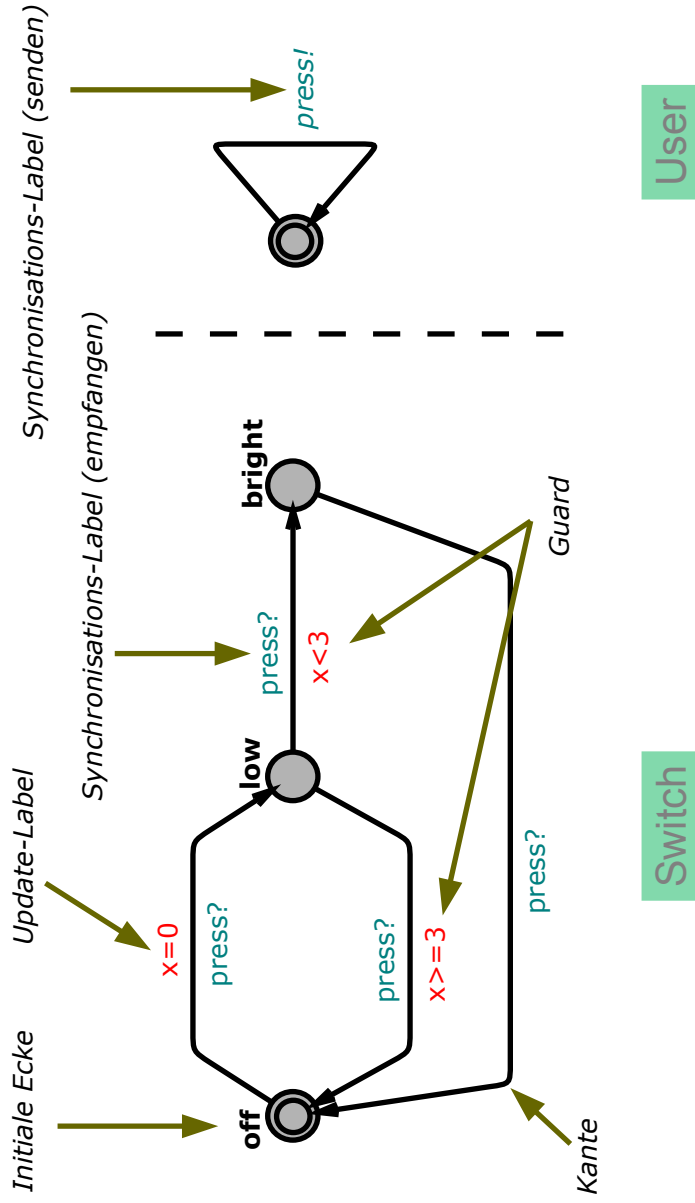




# Timed Automata in UPPAAL – Beispiel Doppelklicklichtschalter

17

- ▶ Achtung: Jetzt mit Realzeit-Variablen, -Guards (Bedingungen)



Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)



# Timed Automata in UPPAAL – Zustände

18

- ▶ Zustände (Ecken, Knoten)
  - Name
  - Invariante: Bedingung die innerhalb des Zustandes immer gelten muss
- ▶ Invariante kann *normal*, *dringend* (*urgent*) oder *verpflichtend* (*committed*) sein
- ▶ **urgent**: Zustand muss ohne Zeitverzögerung wieder verlassen werden
  - Äquivalent: Hinzufügen einer Uhr  $x$ , die auf allen eingehenden Kante auf 0 gesetzt wird, und Invariante  $x \leq 0$
- ▶ **committed**: sobald Zustand verpflichtet, muss der nächste Zustandsübergang Ausgangskante einer verpflichtenden Ecke sein

Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)



Transitionen (Kanten) können folgende Anweisungen enthalten:

- ▶ **Selections:** Zuweisungen, die in Guards und Updates verwendet werden können
- ▶ **Guards:** Bedingungen, unter denen die Kante schalten kann. (z. B. Zeitbedingungen).
- ▶ **Updates:** Wertzuweisungen an Uhren und anderen Variablen.
- ▶ **Synchronisations** über Channels: eine *c!* beschriftete Kante schaltet synchron mit *c?* beschrifteter Kante, wenn
  - beide aktiv sind (d. h. Guards erfüllt)
  - und *c* ein Channel ist

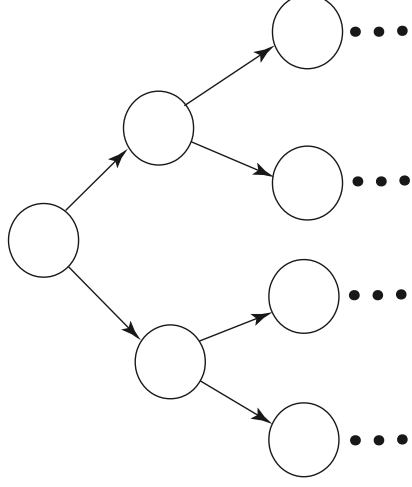
## UPPAAL – Aufbau

- ▶ Automaten werden als Schablonen (*Templates*) modelliert
  - diese werden instanziiert, d.h. parametrisiert werden
  - (Templates sind Fragmentkomponenten, siehe CBSE)
- ▶ Deklarationsteil (textuell)
  - globale und lokale Deklarationen und Definitionen
  - Deklaration von Variablen und Channels
  - Definition von Konstanten und Funktionen
- ▶ Systemdeklarationen:
  - parametrisieren Templates
- ▶ graphischer Teil
  - nutzt Variable etc. aus dem Deklarationsteil

# UPPAAL – Real-time Model-Checking ähnlich zum Model-Checking

21

- ▶ Vom Gesamtsystem wird Berechnungsbaum (oder Zustandsraum) erstellt
- ▶ Enthält alle möglichen Zustände des Systems
- ▶ Wurzel ist der eindeutige Startzustand des Systems
- ▶ Anfragen an den Berechnungsbaum (Queries): Für welche erreichbaren Zustände gilt welches **Prädikat über Realzeitvariablen**?



Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)



# UPPAAL – Query Syntax

22

$\mathbf{E}\langle\langle \varphi, \mathbf{E}[\ ] \varphi, \mathbf{A}\langle\langle \varphi, \mathbf{A}[\ ] \varphi, \varphi \dashrightarrow \psi$

wobei  $\varphi, \psi$  Zustandsformeln über Realzeitvariablen

Seiteneffekt freier Ausdruck, nach *wahr* oder *falsch* auswertbar

$x > 1$

$(P1.Ecke3 \text{ and } (P2.i == 5) \text{ or } (clock > 200))$

not deadlock

**Pfadquantoren:** Auf welchen Pfaden gilt die Aussage?

**A** auf allen Pfaden (all)

**E** auf mindestens einem Pfad (some)

**Temporaloperatoren:** Wann gilt die Aussage?

$\langle\langle$  (**F**) irgendwann entlang des Pfades (*future*)

$[\ ]$  (**G**) in allen Zuständen entlang des Pfades (*globally*)

Leads-To Operator  $\varphi \dashrightarrow \psi$

Gilt  $\varphi$ , so wird in der Zukunft irgendwann  $\psi$  gelten

Kein verschachtelten Pfadquantoren (z. B.:  $\mathbf{A}[\ ] (\mathbf{E}\langle\langle \varphi) )$

Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)

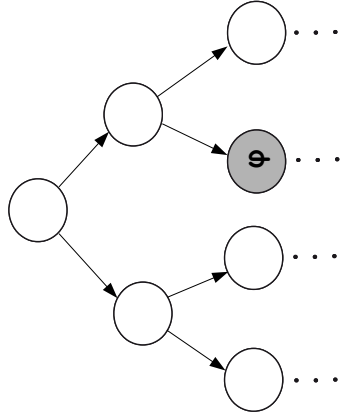


# UPPAAL – Queries: Beispiele (vgl. Standard Model Checking)

23

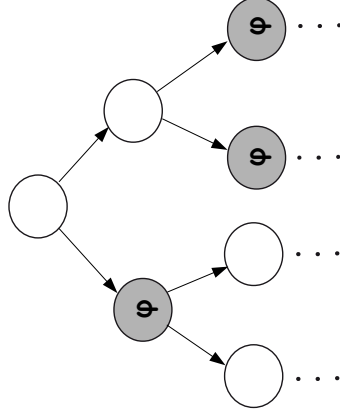
$E\langle\rangle\varphi$  (EF  $\varphi$ )

Exists path with real-time  
Condition eventually



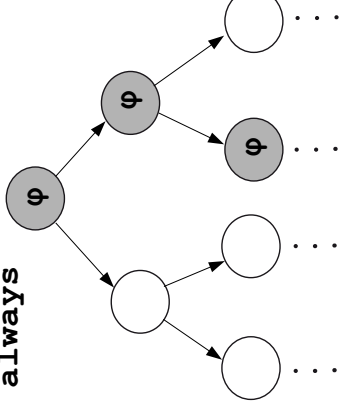
$A\langle\rangle\varphi$  (AF  $\varphi$ )

All paths: with real-time  
condition eventually



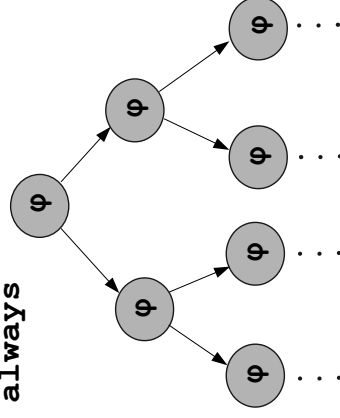
$E[]\varphi$  (EG  $\varphi$ )

Exists path with real-time  
Condition always



$A[]\varphi$  (AG  $\varphi$ )

On all paths: real-time condition  
always



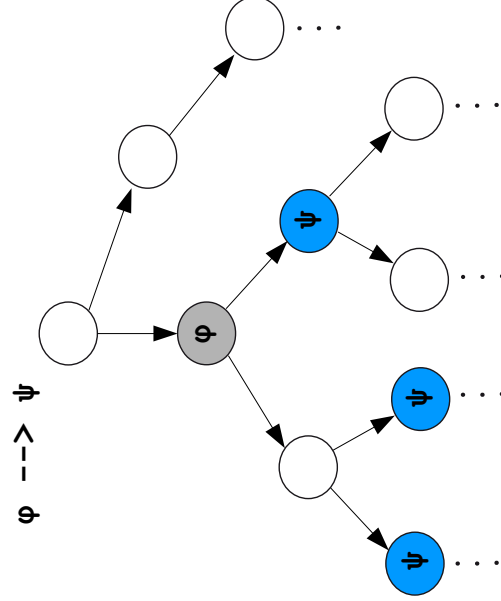
24

# UPPAAL – Queries: Beispiele (2)

Leads-To Operator  $\varphi \dashrightarrow\psi$

Gilt  $\varphi$  in einem Zustand, so wird in der Zukunft irgendwann  $\psi$  gelten

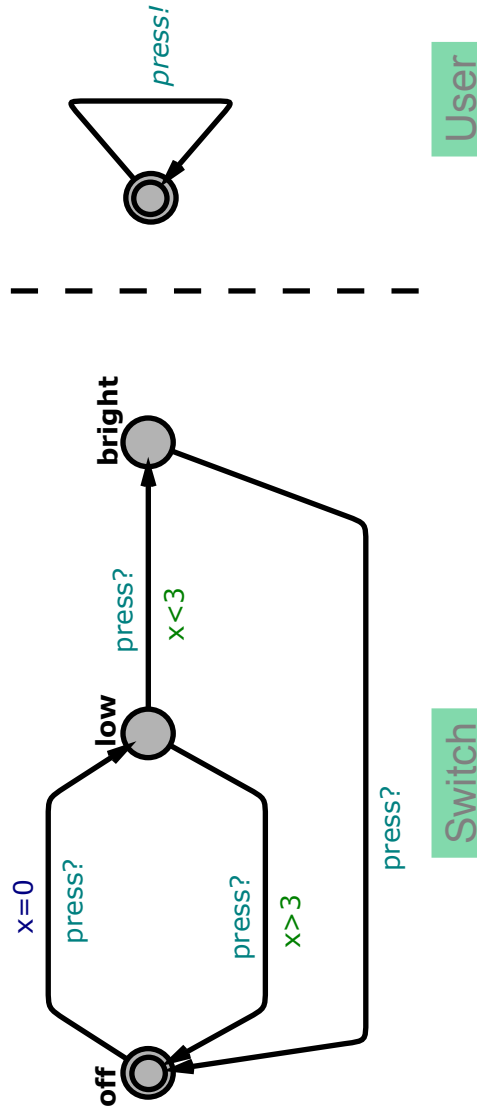
Beispiel: From state with  $\varphi$ , on all paths: holds  $\psi$  eventually



# UPPAAL – Queries: Realzeit-Aussagen über Doppelklickautomat

25

- E ↔ Switch.bright  
Ecke *bright* im Prozess Schalter kann erreicht werden ist erfüllt
- Switch.low → (Switch.off || Switch.bright)  
Ecke *low* wird in jedem Fall verlassen nicht erfüllt, da User nicht zwangsläufig „drückt“
- A[] not deadlock  
Jeder Zustand hat einen Nachfolger



Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)



## Why is Model Checking Important?

26

Finite Automata play an important role in safety-critical software

- ▶ Automotive Software Engineering
- ▶ Controller programming
- ▶ Robot programming
- ▶ Machine2machine communication

Prof. U. Almann, Softwareentwicklungswerkzeuge (SEW)

Besides real-time features also can be verified:  
safety (Ausfallsicherheitseigenschaften), energy (Energieeigenschaften),  
privacy, security (Einbruchschutz)



Some slides courtesy to Martin Rothmann

- ▶ Why is model checking a special form of abstract interpretation?
- ▶ What is a system automaton (Systemautomat)? computation tree (Berechnungsbaum)? Path quantor, temporal quantor? query?
- ▶ What is different from model checking to real-time model checking?