MODEL CHECKING
1 - EINFÜHRUNG

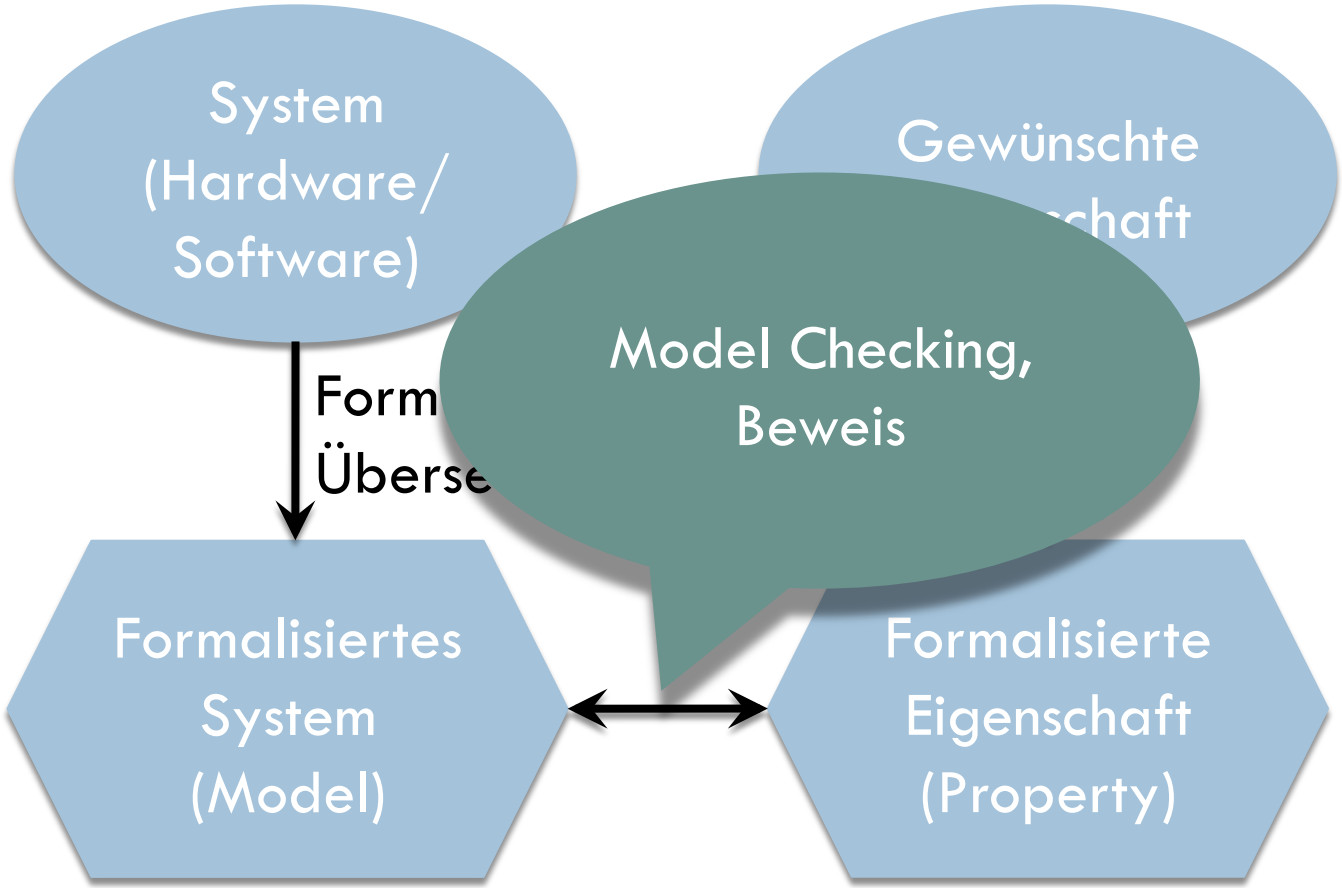
Sommersemester 2009

Dr. Carsten Sinz, Universität Karlsruhe

Software-Qualität

- ***Buggy smartphone software is "new reality"***
  RIM-CEO Jim Balsillie über die fehlerhafte Software des Blackbery Storm (Jan. 2009)
- ***„(...) Software verification (...) has been the Holy Grail of computer science for many decades, but now in some very key areas, for example driver verification, we're building tools that can do actual proofs about the software and how it works in order to guarantee the reliability."***
  Bill Gates, WinHEC 2002

Model Checking



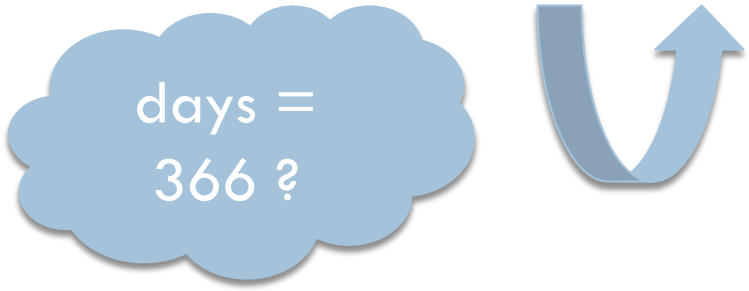
Beispiel 1: Zune Z2K9

"Am 31. Dezember 2008 fielen weltweit alle Zune-Geräte der ersten Generation aus. Ursache war ein interner Fehler bei der Handhabung von Schaltjahren"

Heise Online, 03.01.2009

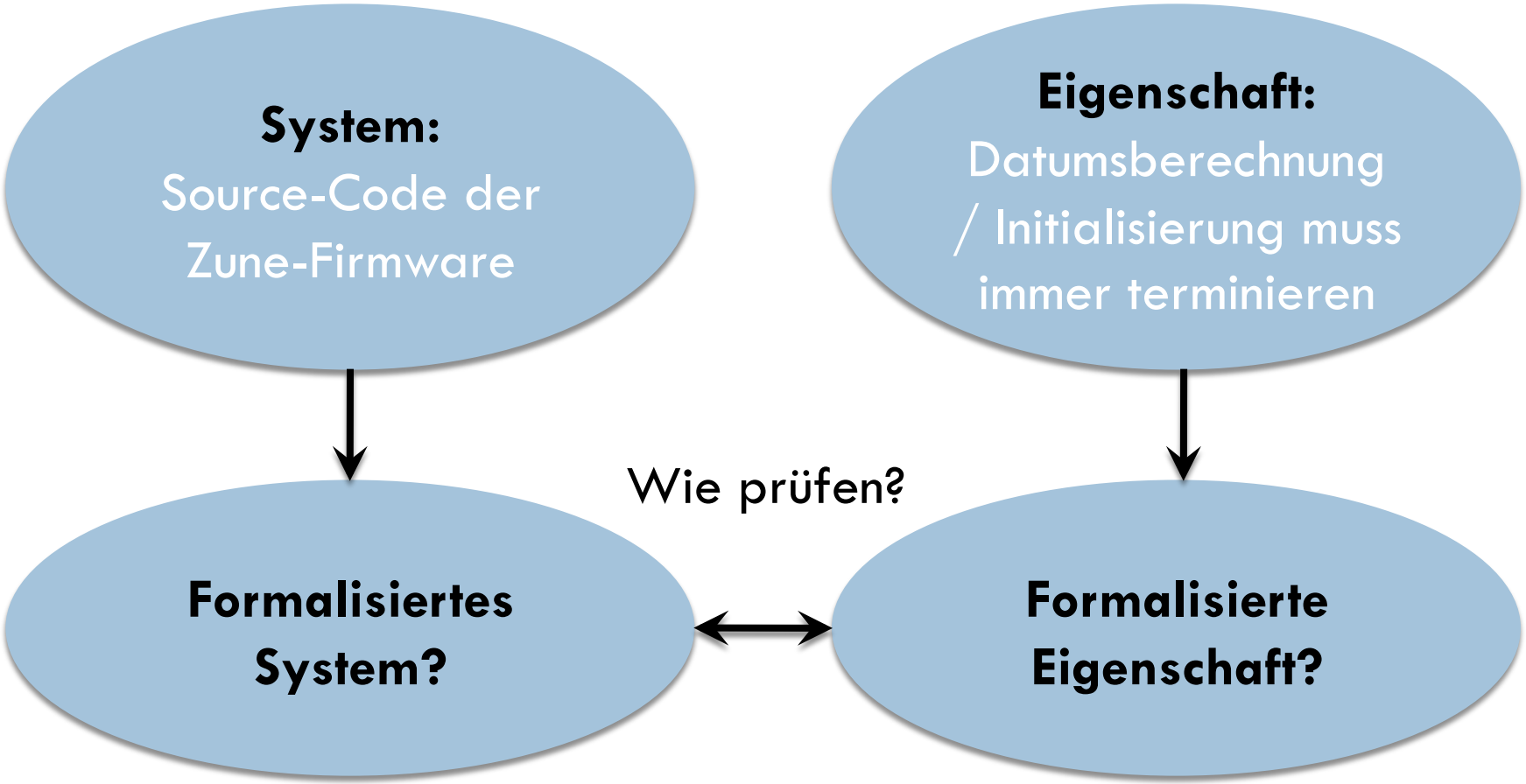
Z2K9: Source Code


```
BOOL ConvertDays(UINT32 days,
     SYSTEMTIME* lpTime)
{
    int dayofweek, month, year;
    UINT8 *month_tab;

    //Calculate current day of the week
    dayofweek = GetDayOfWeek(days);

    year = ORIGINYEAR;
```




```
while (days > 365)
  {
     if (IsLeapYear(year))
     { if (days > 366)
        {
           days -= 366;
           year += 1;
        }
     }
     else
     {
        days -= 365;
        year += 1;
     }
  }
...
```

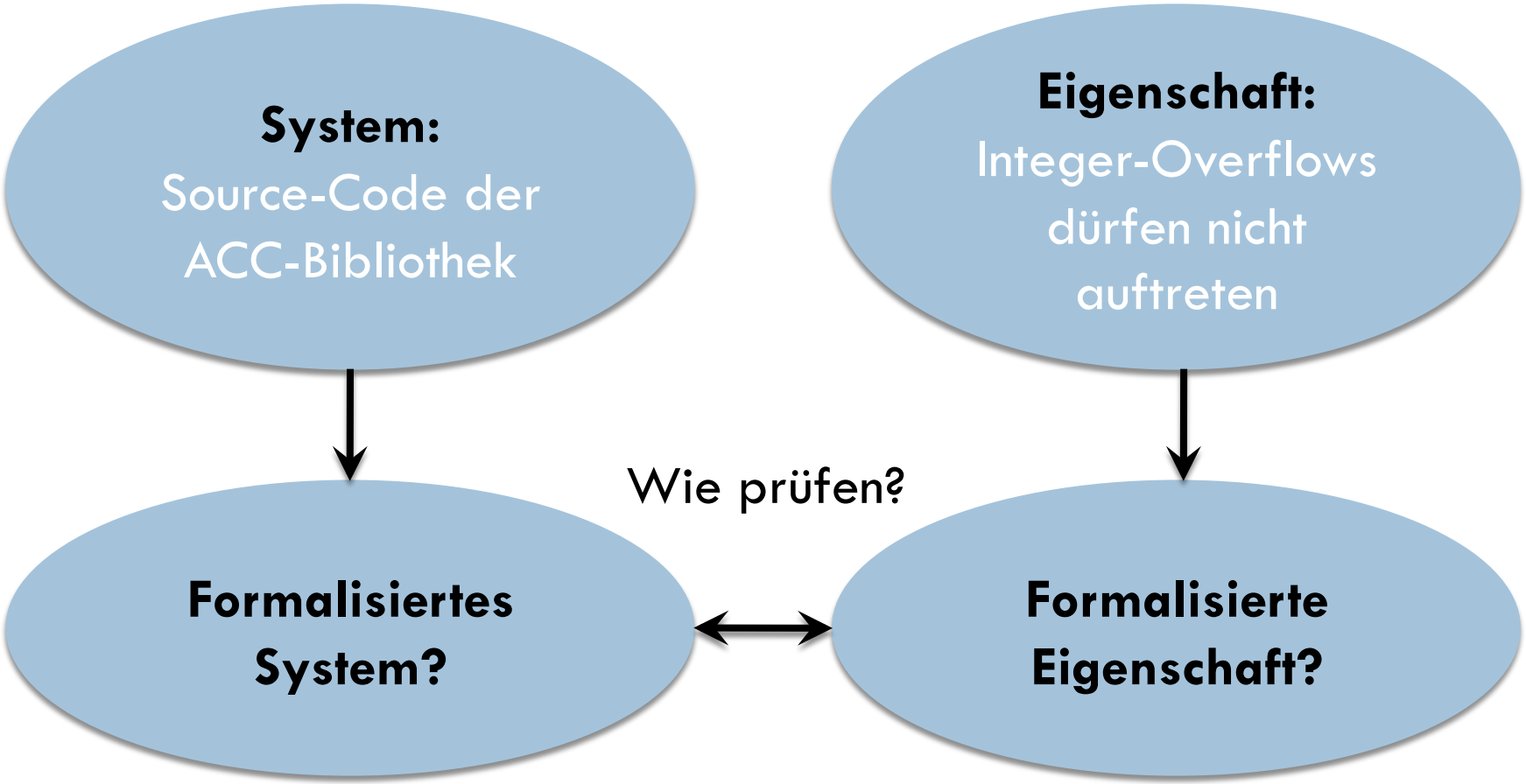
Z2K9: Formalisierung



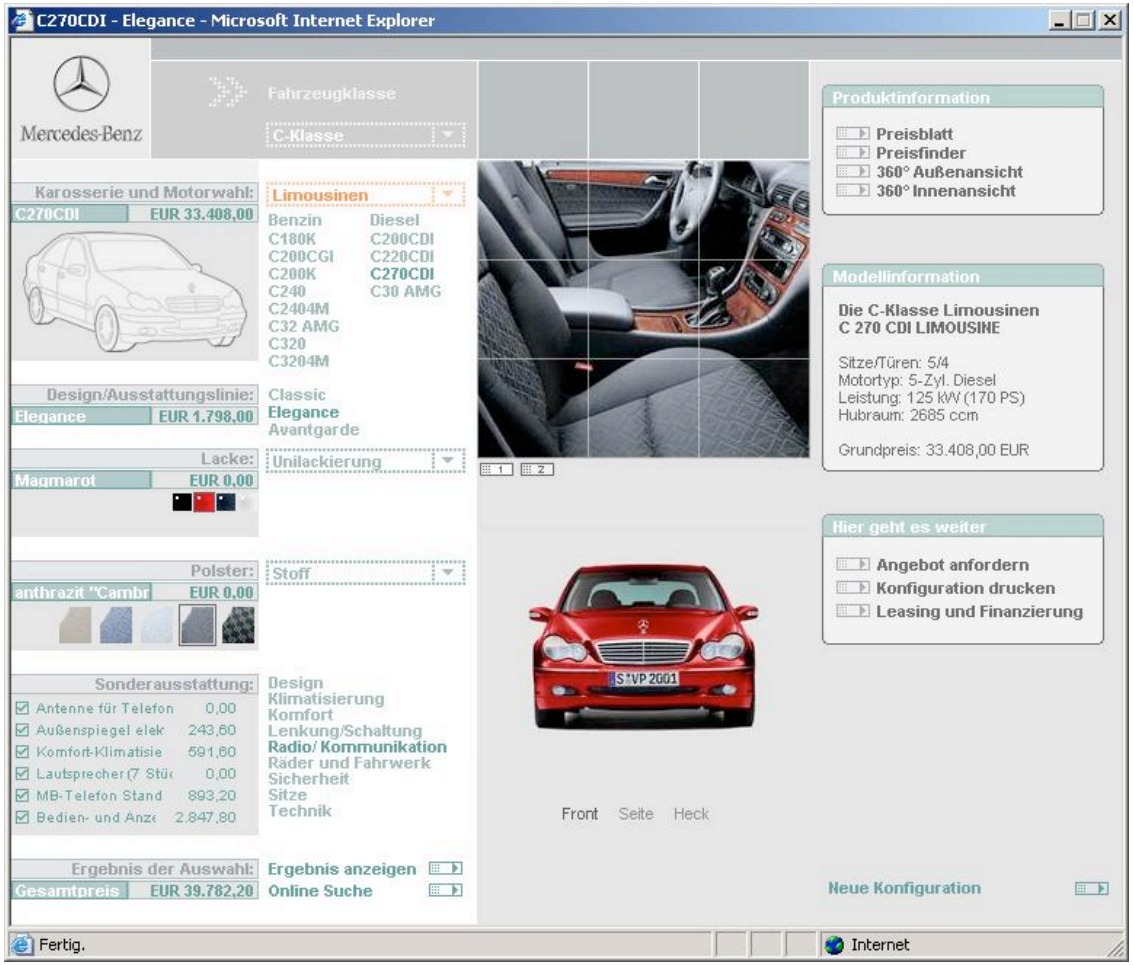
Beispiel 2: Bosch ACC

- Nicht öffentlich verfügbar.

Bosch ACC: Formalisierung



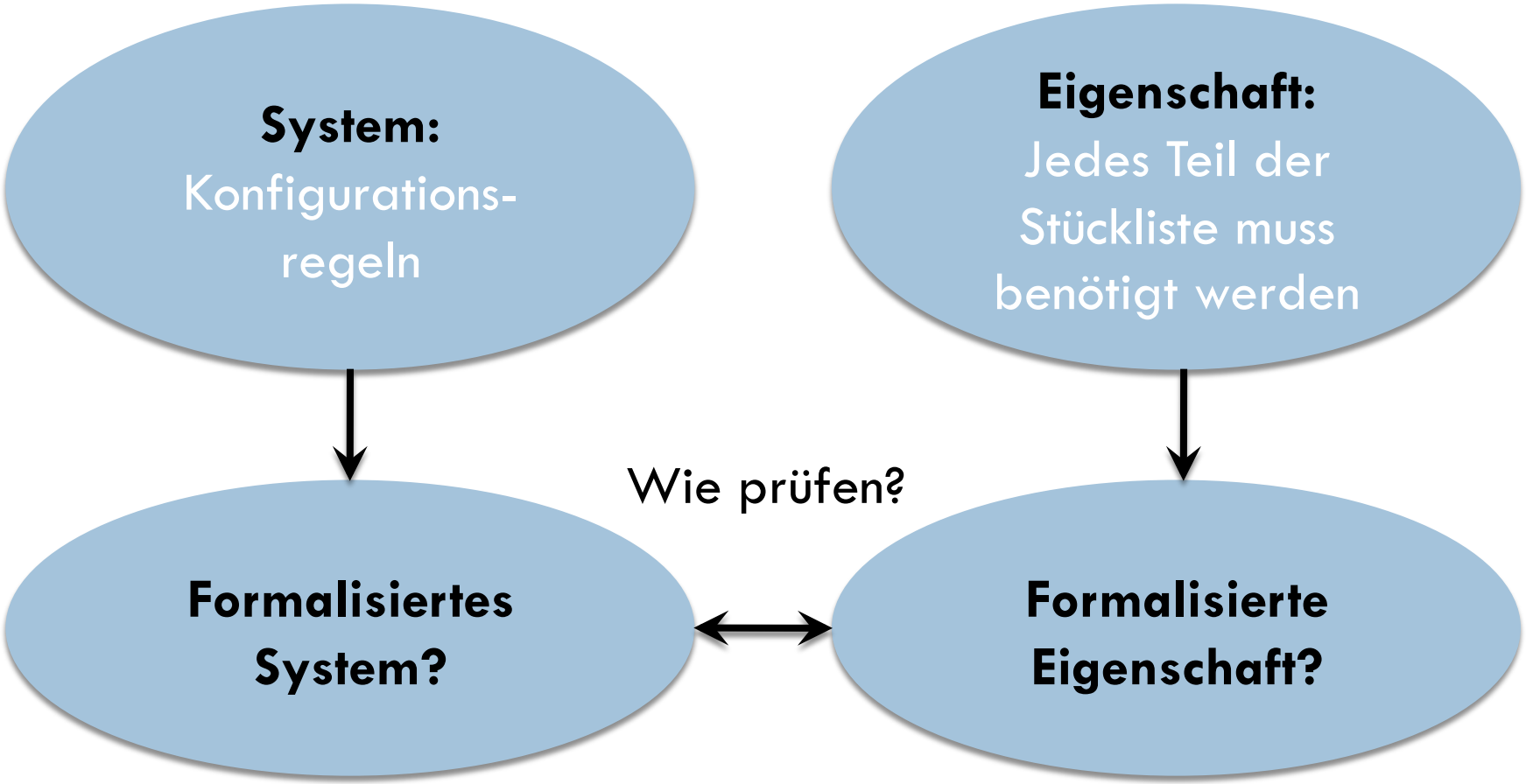
Beispiel 3: Automobil-Konfiguration



Regeln zur Automobil-Konfiguration

- Nicht öffentlich verfügbar.

PKW-Konfiguration: Formalisierung



Vorlesungsinhalte

- Automatentheorie, temporale Logiken (LTL, CTL)
- SAT-Solving und binäre Entscheidungsdiagramme
- Explicit State Model Checking
- Symbolic Model Checking
- Bounded Model Checking
- Software Bounded Model Checking
- Werkzeuge: SPIN, SMV, BLAST, CBMC
- Anwendungen

Organisatorisches

- Übungen:
  - 14-tägig, Do 15:30-17:15, Seminarraum -107
  - Beginn am 06.05.2009
  - Teilnahme an Übungen nicht zwingend, aber empfohlen
- Prüfung:
  - Mündlich, Vertiefungsgebiet: Theoretische Grundlagen
- Literatur:
  - E. Clarke, O. Grumberg, D. Peled: Model Checking (MIT Press, 1999)
  - K. McMillan: Symbolic Model Checking (Kluwer, 1993)