Model Checking

Roderick Bloem,
Bettina Könighofer, Vedad Hadzic
IAIK

Today

Administrative

Motivation

Material & Communications

- **OLD FASHIONED, PHYSICAL LECTURE!**
- **Lecture:** Thursday 4 – 5:30P
- **Practicals:** Right after, only if there is something to discuss
- **Question Hours:** Right after, only if there is something to discuss

- **Webpage:** https://www.iaik.tugraz.at/course/model-checking-705080-sommersemester-2023/
- **Discord:** https://discord.gg/2wY64jUD2P, channel mc (robot)
- **Email:** Vedad.Hadzic@iaik.tugraz.at, Bettina.koenighofer@iaik.tugraz.at roderick.bloem@iaik.tugraz.at

Time Line

Date	Lecture: 4-5:30PM, IFEG042	Exercise: 5:30P,IFEG042
2023-03-09	Intro	
2023-03-16	Modeling Systems – Chapter 3	**Handout** warmup assignment
2023-03-23	SAT-Based Model Checking – Ch. 10	**Tutorial** Z3 Intro
2023-03-30	SAT-Based Model Checking – Ch. 10	**Handout** BMC assignment
2023-04-02		***Deadline*** *Warmup Assignment*
04-06, 04-13	Easter break	
2023-04-20	SAT-Based Model Checking – Ch.10	**Tutorial** Modeling with Yosys, BTOR
2023-04-27	Temporal Logic – Chapter 4	**Handout** k-induction
2023-04-30		***Deadline*** *BMC assignment*
2023-05-04	CTL Model Checking – Chapter 5	
2023-05-11	CTL Model Checking – Chapter 5	
2023-05-18	Ascension	
2023-05-21		***Deadline*** *k-induction*
2023-05-25	LTL Model Checking -Chapter 7	
2023-06-01	LTL Model Checking -Chapter 7	
2023-06-15	Probabilistic Model Checking 1	
2023-06-22	Probabilistic Model Checking 2	
2023-06-29	Research	

How to get a grade?

Lecture: Two options

1. Do weekly homework (by yourself), do a good job. Course grade = homework grade, **OR**
2. Take the exam

(Not happy with homework grade? Take exam!)

Practical:

- Three assignments with point distribution 30/40/30.

737 Max

“The people who wrote the code for the original MCAS system were obviously terribly far out of their league and did not know it” – Gregory Travis, tinyurl.com/4cx8wctc
“The MCAS software didn’t have any basic sanity checks to confirm the data was bad,” – Gregory Travis tinyurl.com/229frw2b
346 deaths

Deductive Verification?

```
{false == false} ↔ {true}
r = false;
{r == ($\bigvee_{j=0}^{-1}$ a[j] == x)} ↔ {r == false}
i = 0;
{r == ($\bigvee_{j=0}^{i-1}$ a[j] == x)}
while(i != n) {
  {(r == ($\bigvee_{j=0}^{i-1}$ a[j] == x)) ∧ i != n}
  {r == ($\bigvee_{j=0}^{i-1}$ a[j] == x)}
  if(a[i] == x) {
    {(r == ($\bigvee_{j=0}^{i-1}$ a[j] == x)) ∧ a[i] == x}
    {(true == ($\bigvee_{j=0}^{i}$ a[j] == x)) ∧ a[i] == x} ↔ {true ∧ a[i] == x} ↔ {a[i] == x}
    r = true;
    {r == ($\bigvee_{j=0}^{i}$ a[j] == x)}
  } else {
   {(r == ($\bigvee_{j=0}^{i}$ a[j] == x)) ∧ a[i] != x} ↔ {(r == ($\bigvee_{j=0}^{i-1}$ a[j] == x)) ∧ a[i] != x}
  }
  {r == ($\bigvee_{j=0}^{i}$ a[j] == x)}
  i = i + 1;
  {r == ($\bigvee_{j=0}^{i-1}$ a[j] == x)}
}
{r == ($\bigvee_{j=0}^{n-1}$ a[j] == x) ∧ i == n} ↔ {r == ($\bigvee_{j=0}^{i-1}$ a[j] == x) ∧ i == n}
{r == ($\bigvee_{j=0}^{n-1}$ a[j] == x)}
```

- (Manual) Proofs
- No diagnostics
- Full specifications
- Concurrency is hard

(But: things have gotten better!)

Automatic Verification!

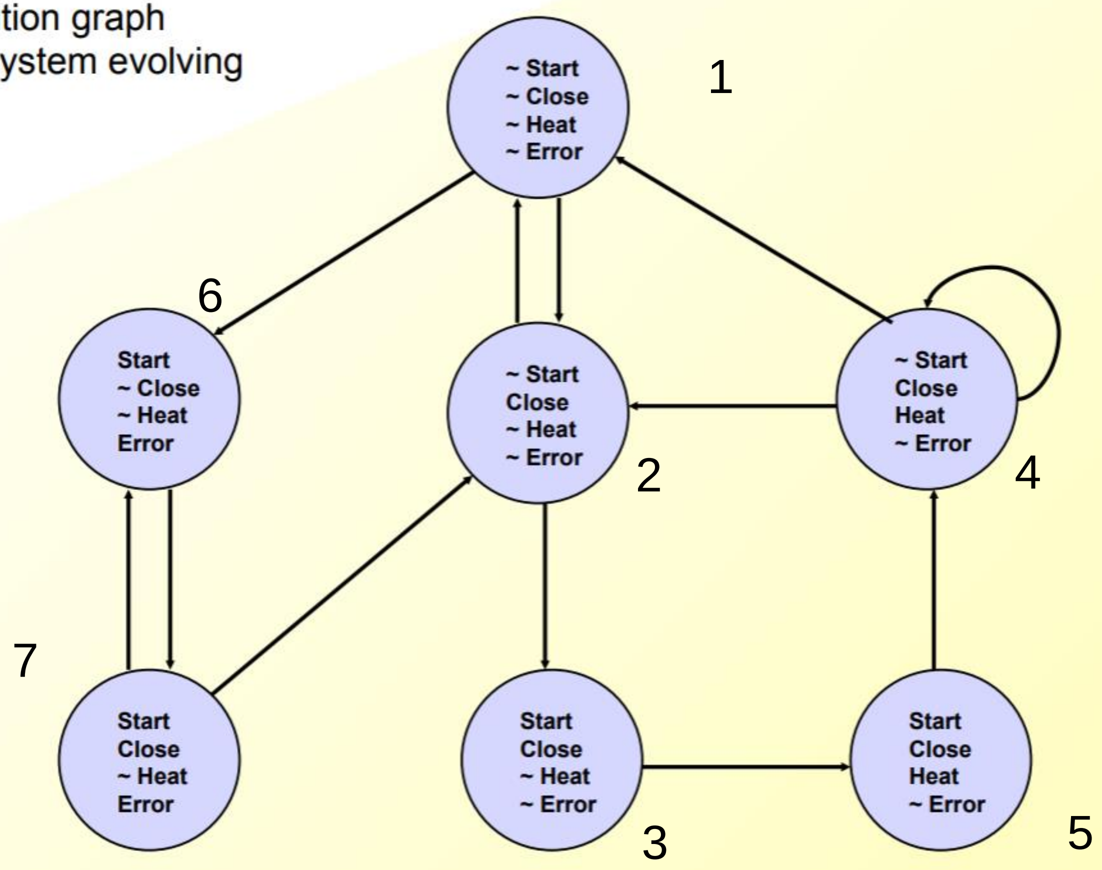
- Program = state machine = graph
- Bug hunting = efficient graph search
- “Interesting” properties = “complicated” graph searches
  - Need language to express interesting things!
- But how to search a graph efficiently?

Ex

Model of computation

Microwave Oven Example

State-transition graph describes system evolving over time.

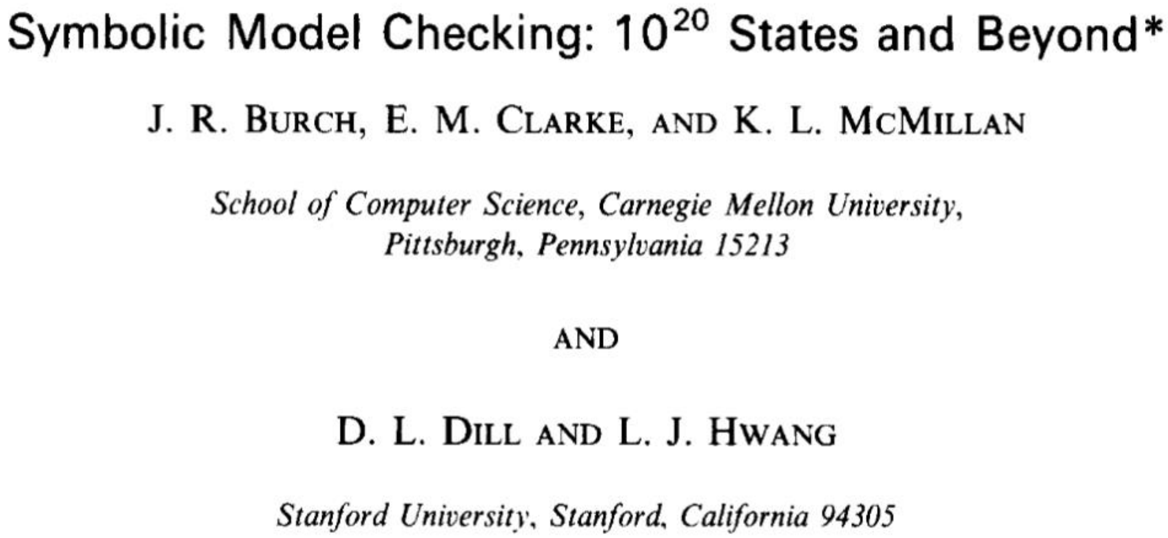


What properties are interesting?

Slide by Ed Clarke

Efficiency

- 1981: EMC Model checker ~10^4 states
- 1992 BDDs:



Symbolic Model Checking: 10^{20} States and Beyond*

J. R. BURCH, E. M. CLARKE, AND K. L. MCMILLAN

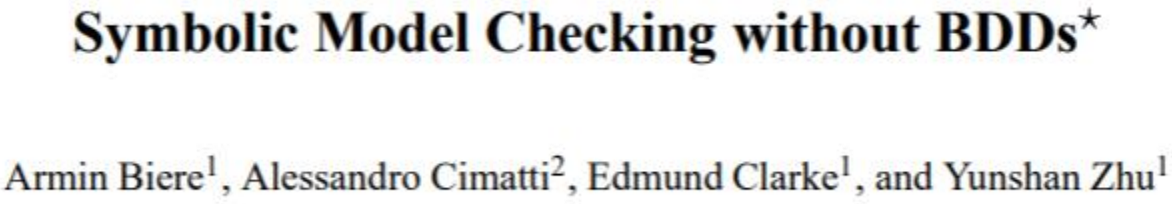
School of Computer Science, Carnegie Mellon University,
Pittsburgh, Pennsylvania 15213

AND

D. L. DILL AND L. J. HWANG

Stanford University, Stanford, California 94305

- 1999 SAT:

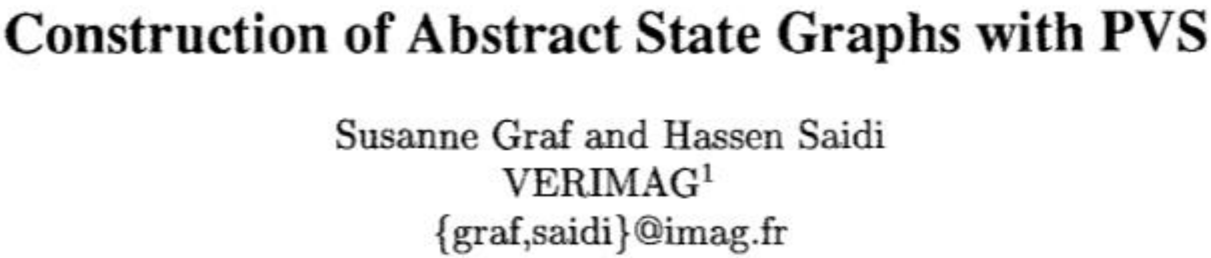


Symbolic Model Checking without BDDs*

Armin Biere[1], Alessandro Cimatti[2], Edmund Clarke[1], and Yunshan Zhu[1]

Efficiency

1992 Abstraction

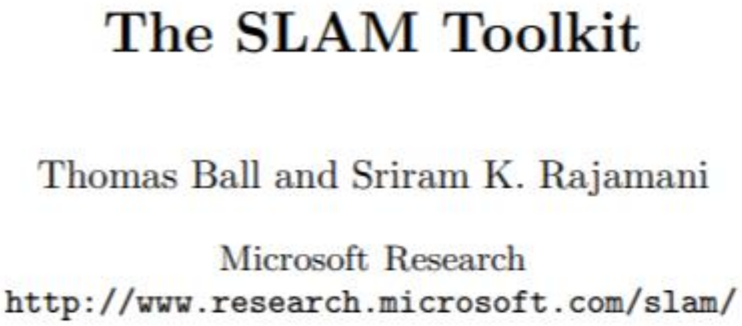


Construction of Abstract State Graphs with PVS

Susanne Graf and Hassen Saidi
VERIMAG[1]
{graf,saidi}@imag.fr

~1995: Partial Order Reduction

~2000: Software



The SLAM Toolkit

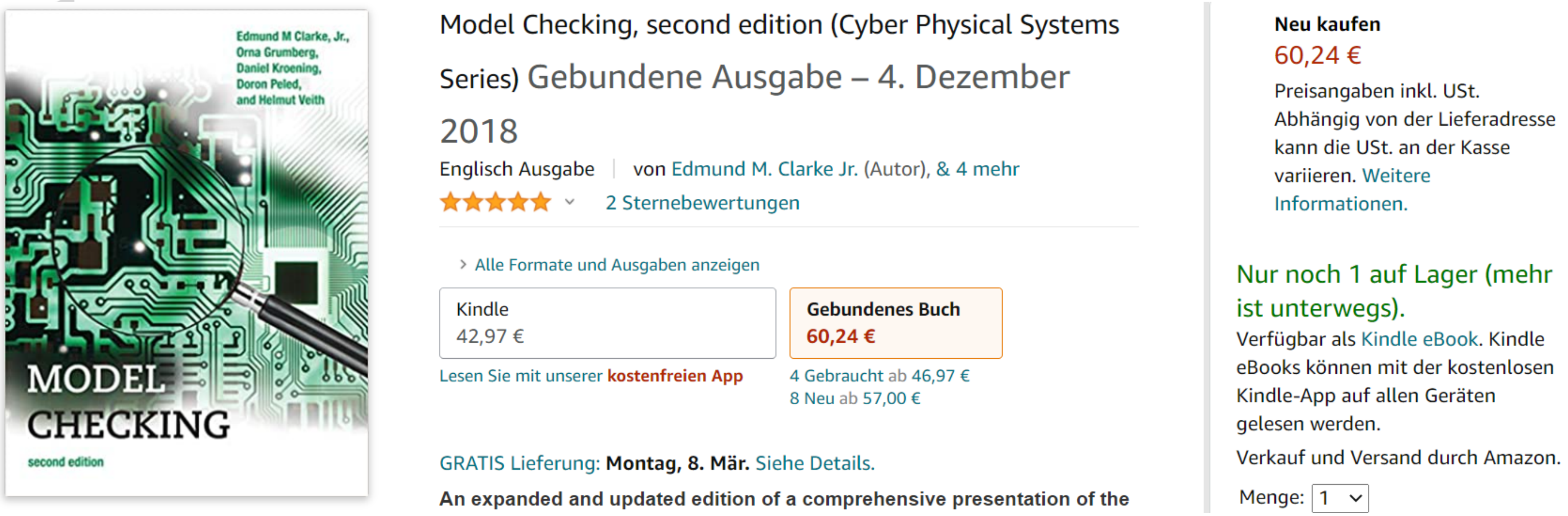
Thomas Ball and Sriram K. Rajamani

Microsoft Research
http://www.research.microsoft.com/slam/

EDMUND M. CLARKE, E. ALLEN EMERSON, JOSEPH SIFAKIS

Model Checking: An Automated Quality Assurance Method

The Book



Model Checking, second edition (Cyber Physical Systems Series) Gebundene Ausgabe – 4. Dezember 2018

Englisch Ausgabe | von Edmund M. Clarke Jr. (Autor), & 4 mehr

★★★★★ 2 Sternebewertungen

› Alle Formate und Ausgaben anzeigen

Kindle 42,97 €	Gebundenes Buch 60,24 €
Lesen Sie mit unserer **kostenfreien App**	4 Gebraucht ab 46,97 € 8 Neu ab 57,00 €

GRATIS Lieferung: **Montag, 8. Mär.** Siehe Details.

An expanded and updated edition of a comprehensive presentation of the

Neu kaufen

60,24 €

Preisangaben inkl. USt. Abhängig von der Lieferadresse kann die USt. an der Kasse variieren. Weitere Informationen.

Nur noch 1 auf Lager (mehr ist unterwegs).

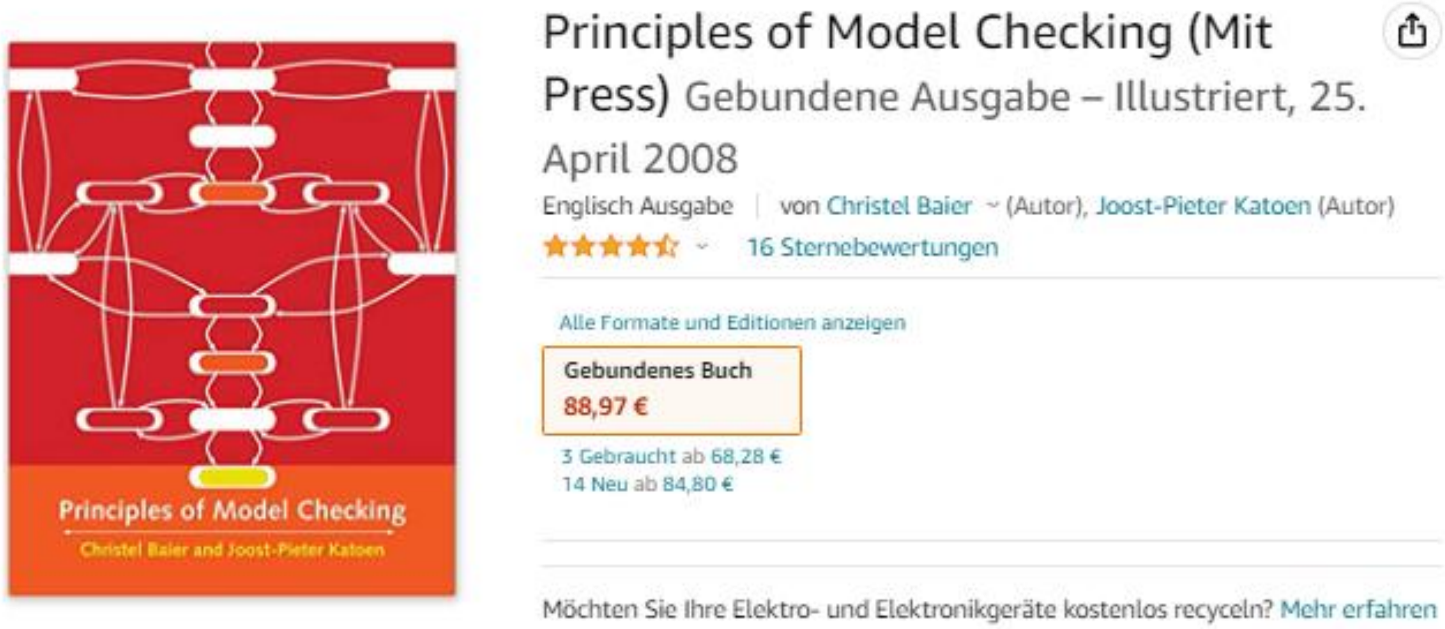
Verfügbar als Kindle eBook. Kindle eBooks können mit der kostenlosen Kindle-App auf allen Geräten gelesen werden.

Verkauf und Versand durch Amazon.

Menge: 1

Clarke, Grumberg, Kroening, Peled, Veith, *Model Checking,* MIT Press 2018 (This is the second edition. The first has a shorter author list.)

The Book



Principles of Model Checking

Christel Baier and Joost-Pieter Katoen

Principles of Model Checking (Mit Press) Gebundene Ausgabe – Illustriert, 25. April 2008

Englisch Ausgabe | von Christel Baier (Autor), Joost-Pieter Katoen (Autor)

★★★★☆ 16 Sternebewertungen

Alle Formate und Editionen anzeigen

Gebundenes Buch
88,97 €

3 Gebraucht ab 68,28 €
14 Neu ab 84,80 €

Möchten Sie Ihre Elektro- und Elektronikgeräte kostenlos recyceln? Mehr erfahren

Baier, Katoen, *Principles of Model checking,* MITPress 2008

Other good books:
Clarke, Henzinger, Veith, Bloem, *Handbook of Model Checking,* Springer 2018