Model Checking

Roderick Bloem,
Bettina Koenighofer, Vedad Hadzic
IAIK

Today

- Motivation
- Administrative

Deductive Verification?

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

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

(But: things have gotten better!)

Automatic Verification!

- Program = finite state machine = graph
- Bug hunting = efficient graph search
- “Interesting” properties = “complicated” graph searches
  - Need language to express interesting things!

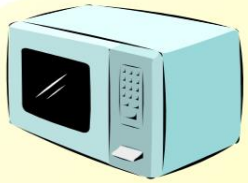
- But how to search a graph efficiently?

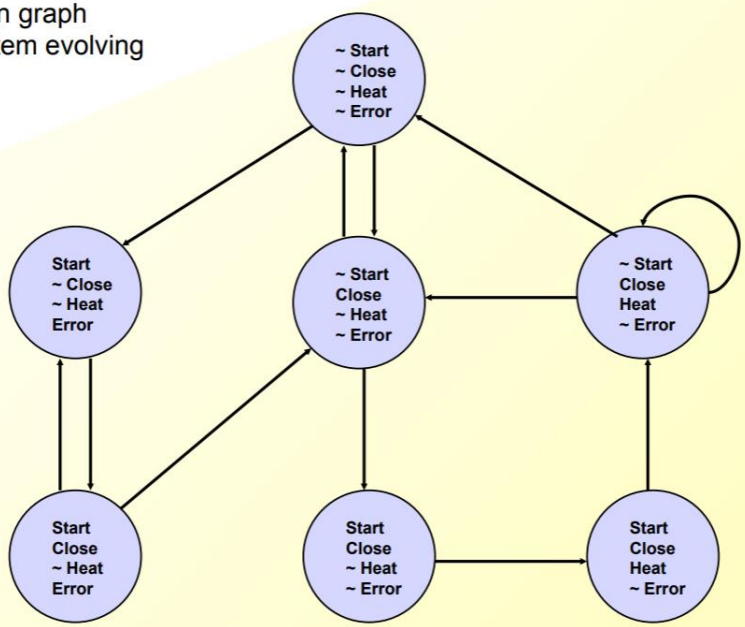
Example

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/


acm
A.M.
TURING
AWARD
2007
EDMUND M. CLARKE, E. ALLEN EMERSON, JOSEPH SIFAKIS
Model Checking: An Automated Quality Assurance Method

Plan

DATE	TOPIC	Teams	Exercise
2021-03-04	Intro	link	
2021-03-11	Chapter 3: Modeling	link	
2021-03-18	Chapter 10: SAT-based Model Checking	link	
2021-03-25	Chapter 10	link	**Exercise Handout**
2021-04-15	Chapter 4: Temporal Logic	link	
2021-04-22	Chapter 5: CTL Model Checking	link	
2021-04-29	Chapter 7: Automata and LTL	link	
2021-05-06	Chapter 7	link	
2021-05-20	Chapter 8: Binary Decision Diagrams	link	
2021-05-27	Chapter 11: Equivalences and Preorders	link	
2021-06-10	Chapter 12: Partial Order Reduction	link	
2021-06-17	Chapter 13: Abstraction	link	
2021-06-24	?	link	

Material & Communications

- **Lecture:** Thursday 4 – 5:30P
- **Practicals:** Thursday 5:30P (if there is anything to tell)
- **Question Hours:** Tuesday 10 AM

- **Webpage:** https://www.iaik.tugraz.at/course/model-checking-705080-sommersemester-2021/
- **Discord:** TBD
- **Newsgroup:** no. Discord!
- **Email:** Vedad.Hadzic@iaik.tugraz.at, Bettina.koenighofer@iaik.tugraz.at roderick.bloem@iaik.tugraz.at

How to get a grade?

Lecture: Two options

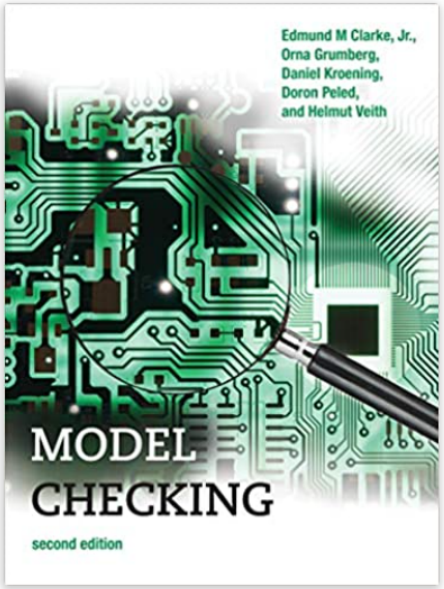
1. Do weekly homework (by yourself), do a good job. Course grade = homework grade, **OR**
2. Take the exam

(Not happy with homework grade? Take exam!)

Practical:

- 2 assignments
- At least one submission & you'll get a grade

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	**Gebundenes Buch**
42,97 €	**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.)

Other good books:
Clarke, Henzinger, Veith, Bloem, *Handbook of Model Checking,* Springer 2018
Baier, Katoen. *Principles of Model Checking,* MIT Press, 2008