Model Checking

Lecture:

Roderick Bloem, Bettina Könighofer, Stefan Pranger

Practicals:

Vedad Hadžić, Johannes Haring

Today

- Administrative
- Motivation

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”.
346 deaths

Deductive Verification?

```
r = false;
i = 0;
while(i != n) {

  if(a[i] == x) {

    r = true;
  } else {
  }
  i = i + 1;
}
```

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!

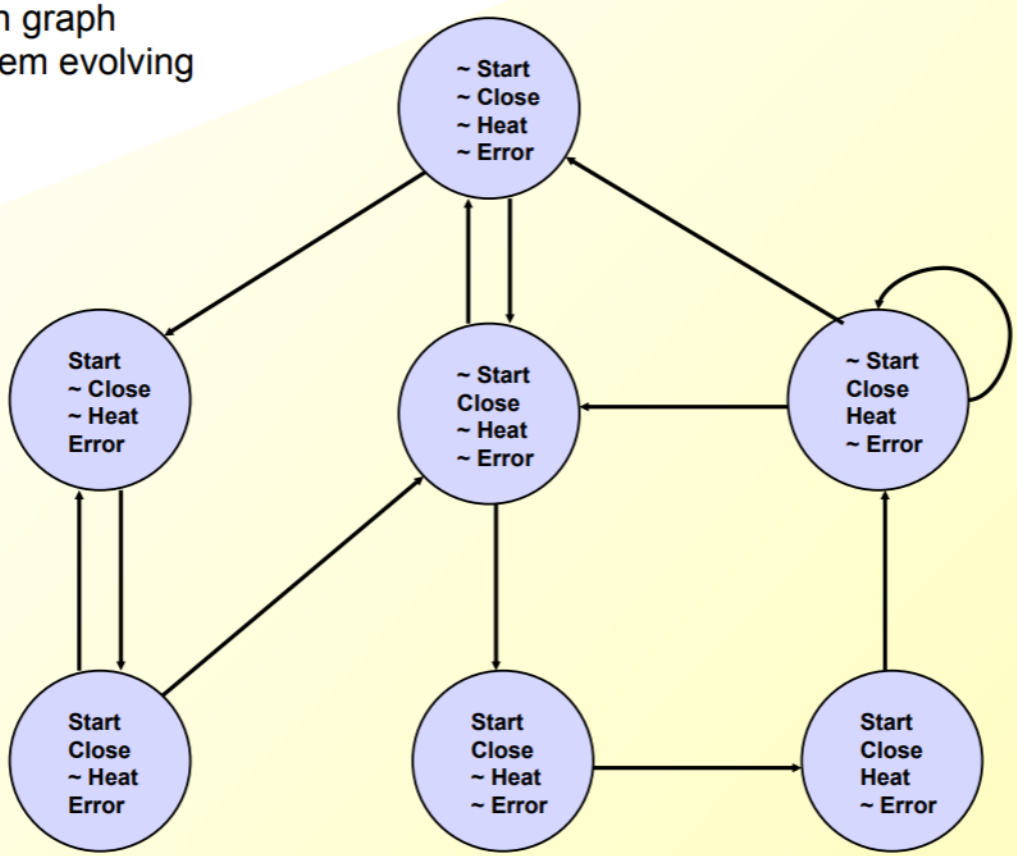
- Program = state machine = graph
- Bug hunting = efficient graph search
- “Interesting” properties = “complicated” graph searches
  - Need language to express interesting things!

- But how to search a graph efficiently?

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

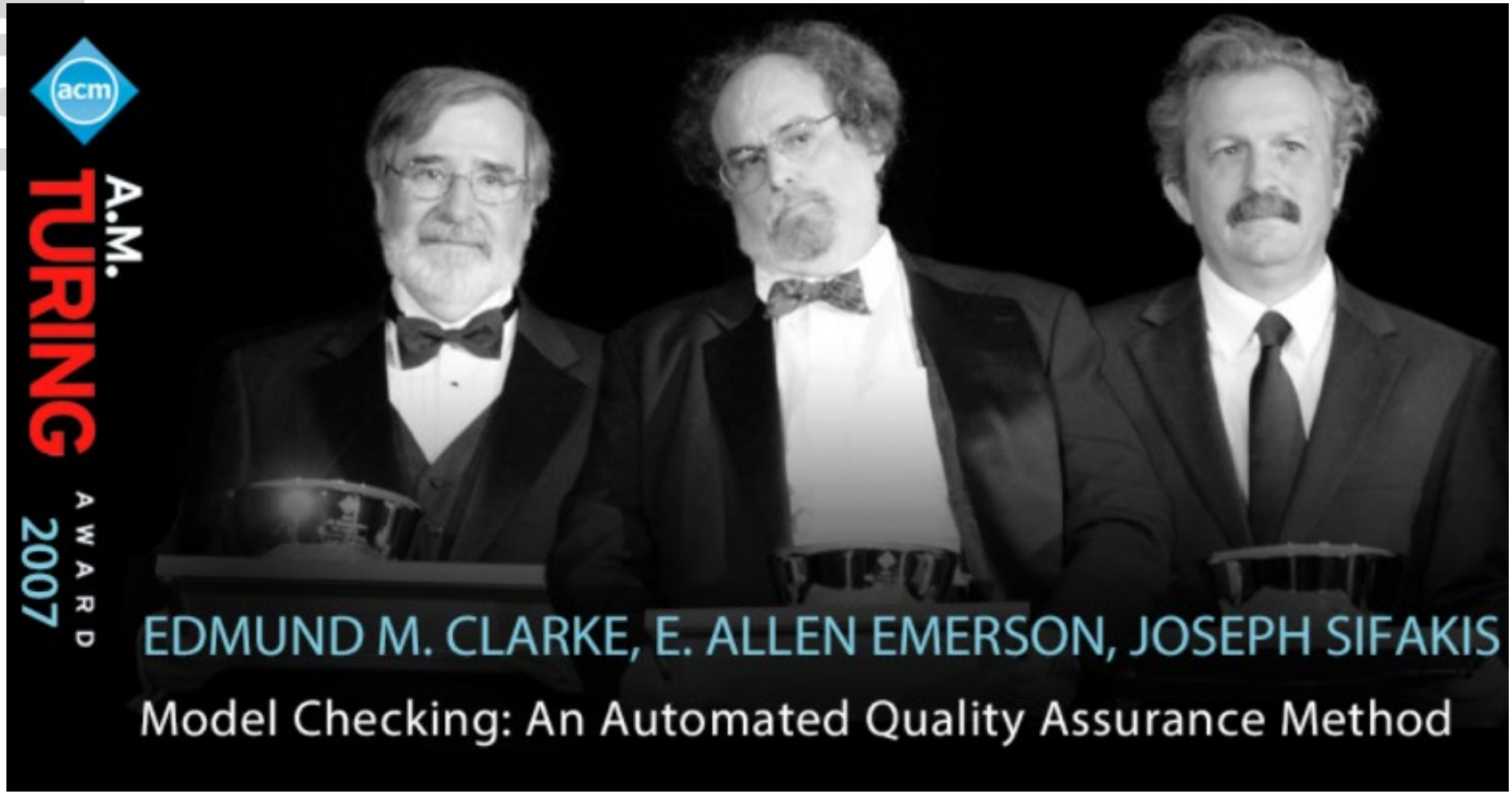
The SLAM Toolkit

Thomas Ball and Sriram K. Rajamani

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

More than Microwave Ovens?

- Amazon Web Services
  - S3, DynamoDB, EBS, lock manager
  - https://assets.amazon.science/67/f9/92733d574c11ba1a11bd08bfb8ae/how-amazon-web-services-uses-formal-methods.pdf
- Facebook
  - Static Analysishttps://research.facebook.com/publications/moving-fast-with-software-verification/
- Intel
  - Security https://community.cadence.com/cadence_blogs_8/b/breakfast-bytes/posts/formally-verifying-processor-security
- Microsoft
  - Device drivers
  - Smart contracts
  - Z3
- Cadence & Synopsys
  - Jasper Formal Verification, VC Formal

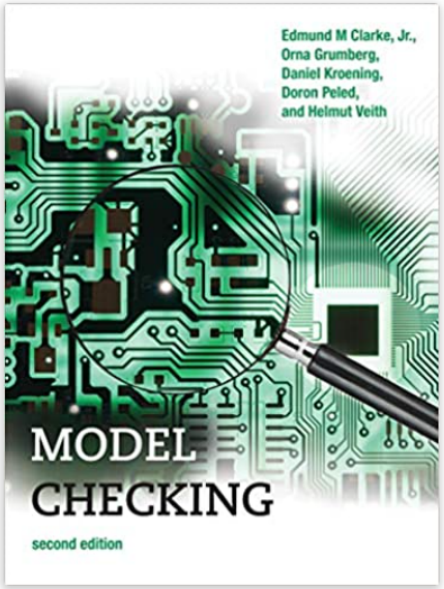

acm
A.M.
TURING
AWARD
2007
EDMUND M. CLARKE, E. ALLEN EMERSON, JOSEPH SIFAKIS
Model Checking: An Automated Quality Assurance Method

Material & Communications

OLD FASHIONED, PHYSICAL LECTURE!
Lecture: Monday 9-10:30, IFEG042 (Seminar Room IAIK)
Practicals: Right after, only if there is something to discuss
Question Hours: Monday after class.

Webpage: https://www.iaik.tugraz.at/course/model-checking-705080-sommersemester-2024/
Discord: https://discord.gg/FDcxjR728N, Channel MC (robot)
Email: bettina.koenighofer@iaik.tugraz.at, roderick.bloem@iaik.tugraz.at, stefan.pranger@iaik.tugraz.at johannes.haring@iaik.tugraz.at, vedad.hadzic@iaik.tugraz.at

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.

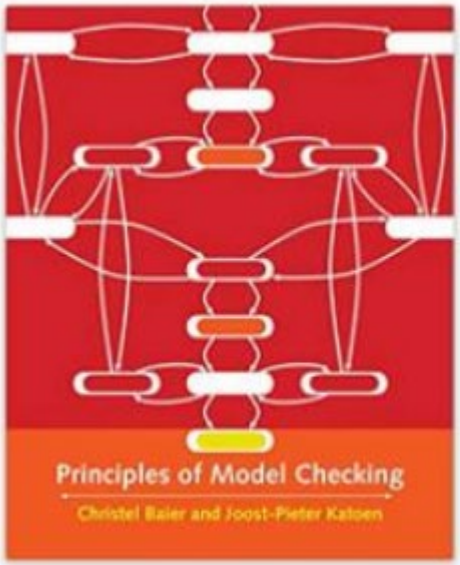
An expanded and updated edition of a comprehensive presentation of the

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.)

The Book



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

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

★★★★½ 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,* MIT Press, 2008

Another good book:
Clarke, Henzinger, Veith, Bloem, *Handbook of Model Checking,* Springer 2018

How to get a grade?

Lecture: Two options

1. Do an exam, **or**
2. Participate in class, and do weekly homework. Course grade = homework grade

(Not happy with homework grade? Take exam!)

Details:

- Miss at most 2 classes
- Skip at most 2 homeworks

Practical:

- Individual work
- Three assignments with point distribution 30/40/30
- Final interviews

Homework

- Weekly homework
  - uploaded just before the lecture
  - deadline start of the next lecture
- **Individually** or **groups of two**.
  - You can do each homework with a different group.
- Submission
  - In TeachCenter
  - If handwritten, use **clear writing** and a good scan
- Marks
  - available within 1 week of submission deadline at https://cloud.tugraz.at/index.php/s/zeEgt8ptcRQCXEW
  - Final mark = **average of all homework** (even those you do not hand in).
  - You can skip homework **at most 2** weeks.

- Questions
  - email: filip.cano@iaik.tugraz.at
  - I also actively answer questions in the discord channel

Lecture Schedule

Date	Topic	Lecturer
11.03.2024	Intro	Roderick
18.03.2024	SAT-Based Model Checking (BMC, k-induction) – Chapter 10	Roderick
08.04.2024	SAT-Based Model Checking (interpolation) -Chapter 10	Roderick
15.04.2024	SAT-Based Model Checking (PDR) – Chapter 10	Roderick
22.04.2024	Temporal Logic – Chapter 4	Bettina
29.04.2024	CTL Model Checking – Chapter 5	Bettina
06.05.2024	CTL Model Checking – Chapter 5	Bettina
13.05.2024	LTL Model Checking -Chapter 7	Bettina
27.05.2024	Probabilistic Model Checking – Chapter 10 – PRISM & Reachability in Markov Chains	Stefan
03.06.2024	Probabilistic Model Checking – Chapter 10 – PCTL and MDPs	Stefan
10.06.2024	Probabilistic Model Checking – Tempest and Shielded Reinforcement Learning	Stefan
17.06.2024	Reserved slot	---

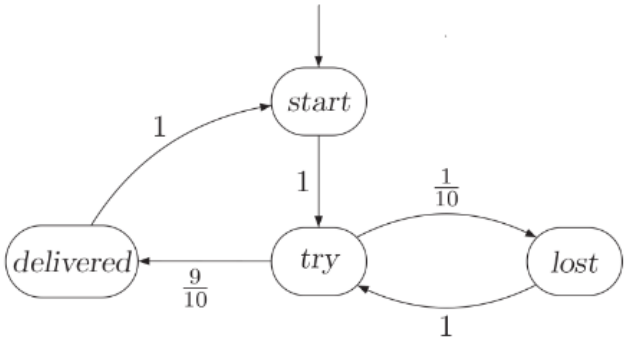
Practicals Schedule

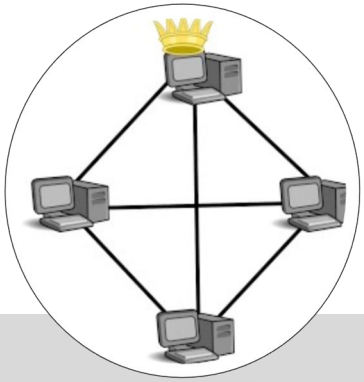
Date	Type	Topic	Lecturer
11.03.2024	Lecture	Intro	Roderick
18.03.2024	Handout	Warmup Exercise	Vedad
08.04.2024	Tutorial	Introduction to Z3	Vedad
15.04.2024	Handout	BMC Exercise	Vedad
21.04.2024	Deadline	Warmup Deadline	—
22.04.2024	Tutorial	Hardware and Verilog	Vedad
29.04.2024	Question Hour	Question Hour BMC	Vedad
06.05.2024	Handout	K-Induction Exercise	Vedad
12.05.2024	Deadline	BMC Deadline	—
13.05.2024	Question Hour	Question Hour K-Induction	Vedad
27.05.2024	Question Hour	Question Hour K-Induction	Vedad
02.06.2024	Deadline	K-Induction Deadline	—

Why do we need Probabilities?

- Analysis of Reliability
  - Probability of Failure,
  - Quanitify Message Loss,
  - Quanitify Arrival Times, …
- Models of Safety-Critical Systems,
  - Modelling Unknowns,
  - Modelling Faults, …
- Analysis of Randomized Algorithms,

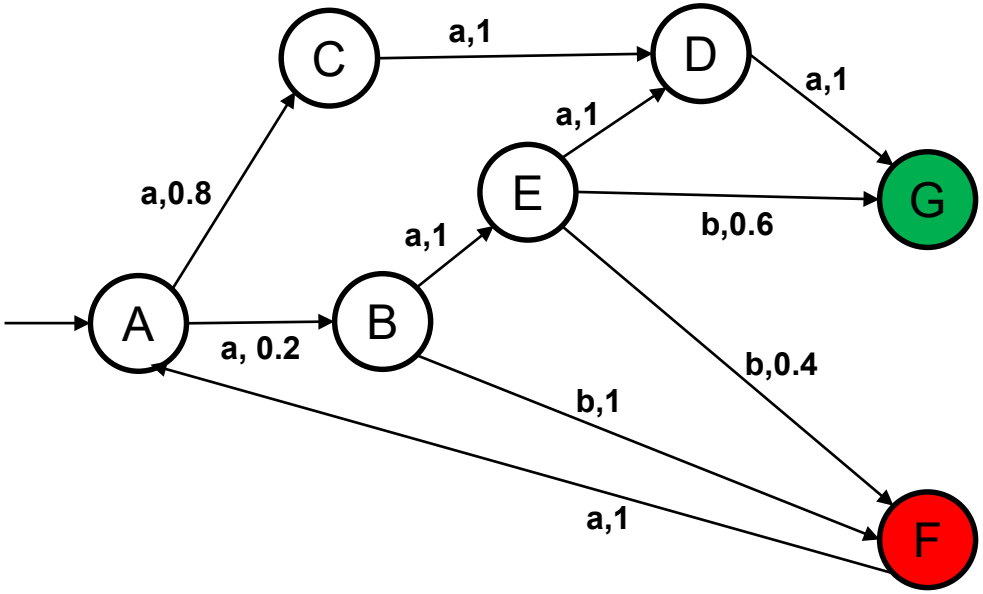
…





Probabilistic Model Checking

- Extend Models with Probabilistic Transitions
- ”Markov Models”

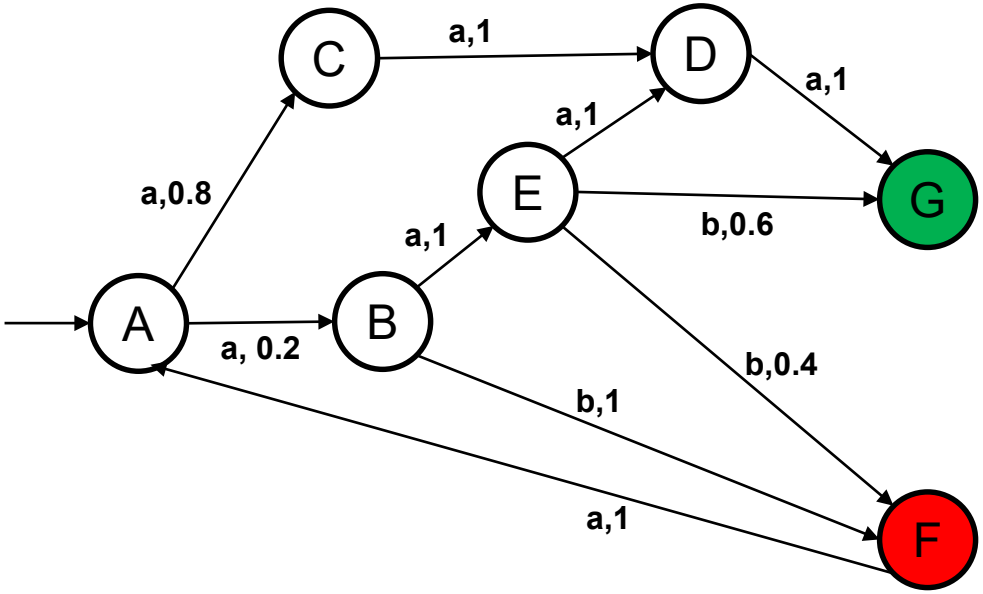


Probabilistic Model Checking

- Formalism to quantify Probabilities

$$P_{\leq 0.95}\,(F \rightarrow \text{true}\ U^{<9} G)$$

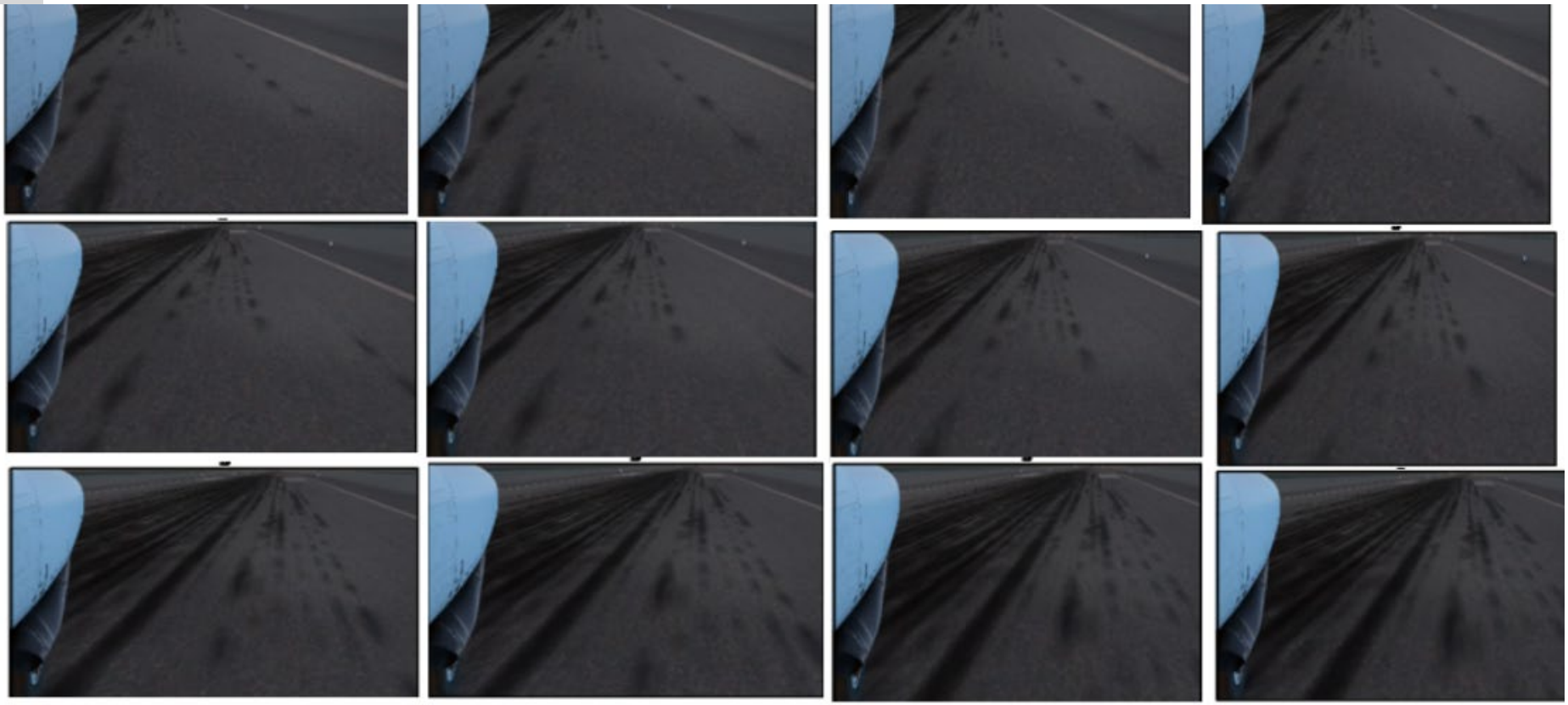
Is the probability of delivering a message withing 9 steps after encountering a failure greater or equal 0.95?



A Probabilistic Model

- Model containing:
  - System Dynamics
  - Controller Decisions
- $P_{<0.01}\ (\boldsymbol{F}\ dist(airplane, centerline) < 200)$?

Perception is hard to model!



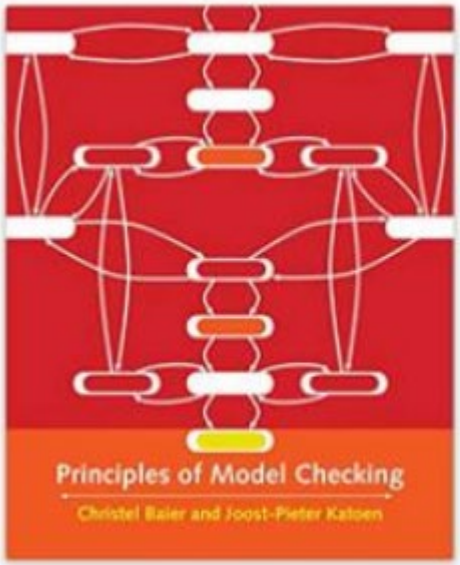
Topics

Book

- Different Markovian Models,
  - *and* how to compute probabilities of events.
- Modelling Language,
  - *and how to use a probabilistic model checker, and*
- pMC in practice.

storm & tempest

The Book



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

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

★★★★½ 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,* MIT Press, 2008

Another good book:
Clarke, Henzinger, Veith, Bloem, *Handbook of Model Checking,* Springer 2018

Lecture Schedule

Date	Topic	Lecturer
11.03.2024	Intro	Roderick
18.03.2024	SAT-Based Model Checking (BMC, k-induction) – Chapter 10	Roderick
08.04.2024	SAT-Based Model Checking (interpolation) -Chapter 10	Roderick
15.04.2024	SAT-Based Model Checking (PDR) – Chapter 10	Roderick
22.04.2024	Temporal Logic – Chapter 4	Bettina
29.04.2024	CTL Model Checking – Chapter 5	Bettina
06.05.2024	CTL Model Checking – Chapter 5	Bettina
13.05.2024	LTL Model Checking -Chapter 7	Bettina
27.05.2024	**Probabilistic Model Checking – Chapter 10 – PRISM & Reachability in Markov Chains**	Stefan
03.06.2024	**Probabilistic Model Checking – Chapter 10 – PCTL and MDPs**	Stefan
10.06.2024	**Probabilistic Model Checking – Tempest and Shielded Reinforcement Learning**	Stefan
17.06.2024	Reserved slot	---