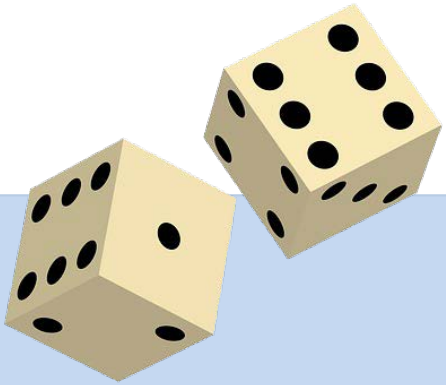
iCyPhy

Software Design for Cyber-Physical Systems

Edward A. Lee



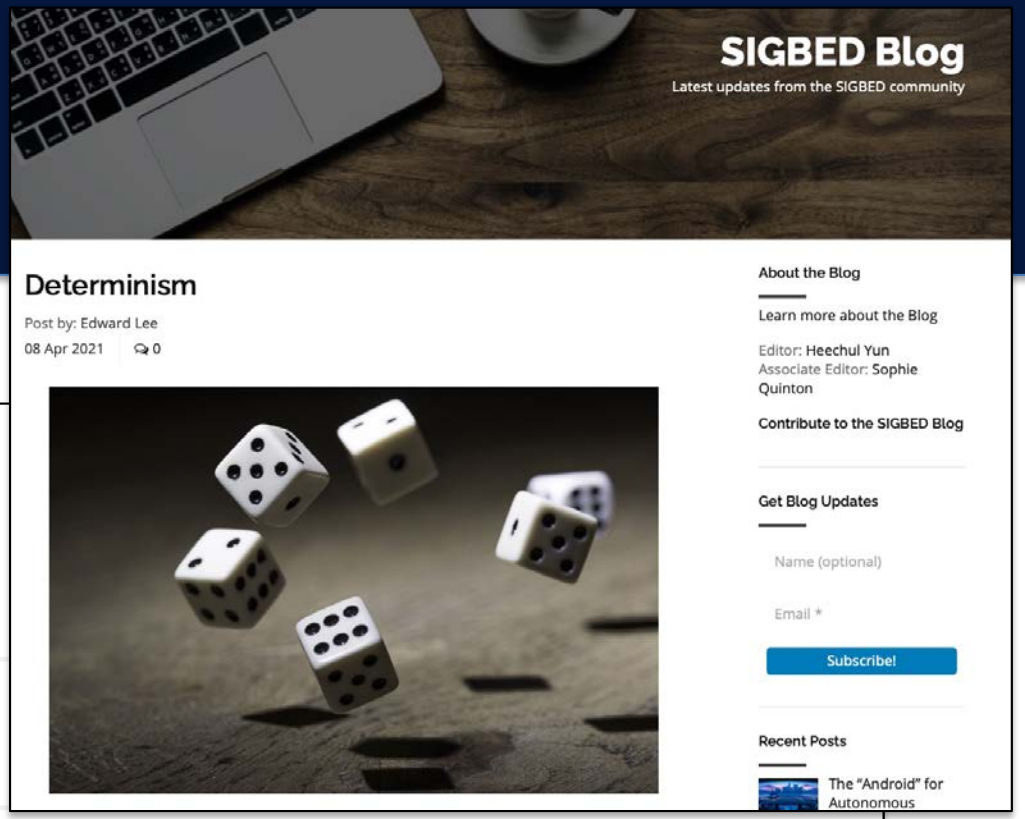
Module 3: Determinism

Technical University of Vienna

Vienna, Austria, May 2022

University of California, Berkeley

Primary References



RESEARCH-ARTICLE OPEN ACCESS

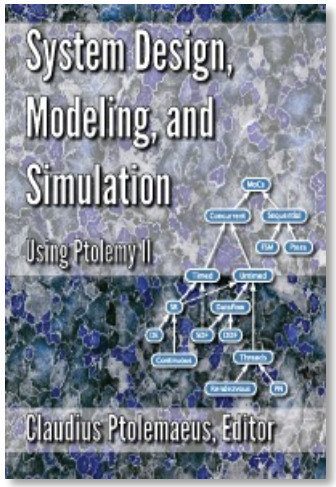
Determinism

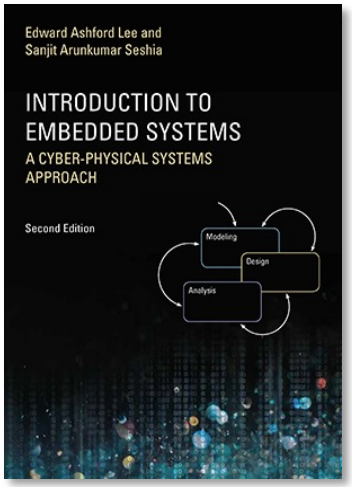
Author: Edward A. Lee Authors Info & Affiliations

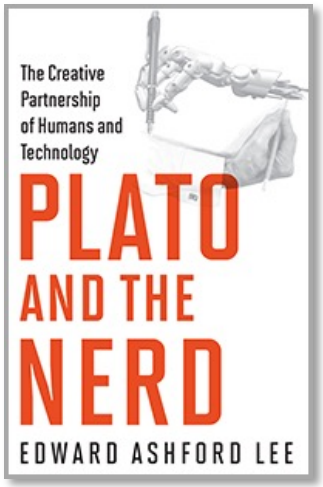
ACM Transactions on Embedded Computing Systems, Volume 20, Issue 5 • July 2021 • Article No.: 38, pp 1–34 • https://doi.org/10.1145/3453652

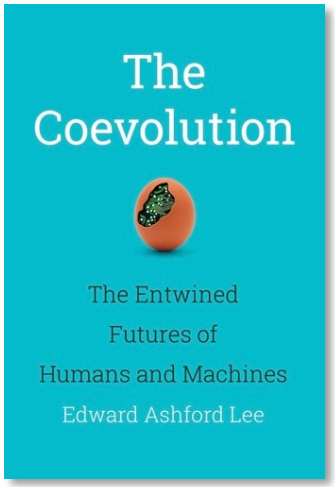
http://ptolemy.org/~eal
eal@berkeley.edu

http://repo.lf-lang.org
Lingua Franca









Terminology in Physics and Philosophy

Determinism: every action is a consequence of preconditions and fixed rules.

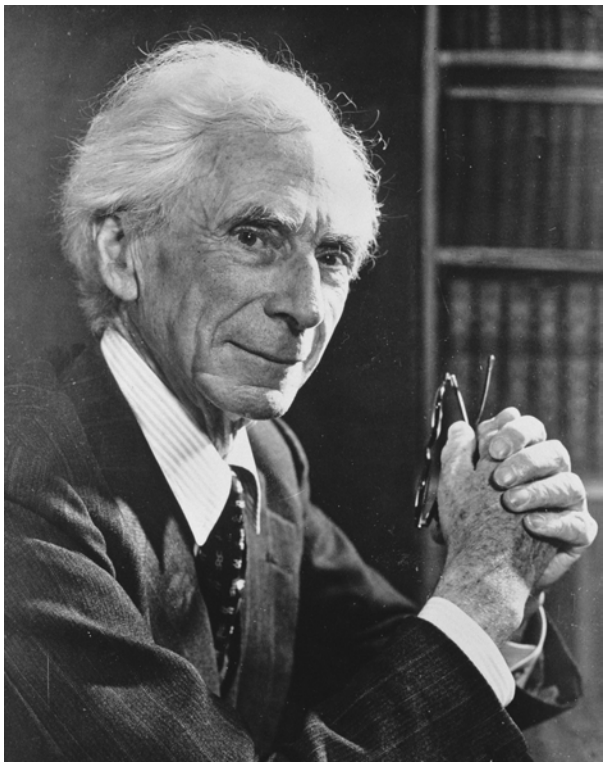
Causation: preconditions *cause* the consequences.

Distaste for nondeterminism in the physical world follows from a distaste for uncaused action.

Causation

"All philosophers, of every school, imagine that causation is one of the fundamental axioms or postulates of science, yet, oddly enough, in advanced sciences such as gravitational astronomy, the word "cause" never occurs … The law of causality, I believe, like much that passes muster among philosophers, is a relic of a bygone age, surviving, like the monarchy, only because it is erroneously supposed to do no harm."

Bertrand Russell (1913)



Difficulties

"This is already enough to make strong the suspicion that a real understanding of determinism cannot be achieved without simultaneously constructing a comprehensive philosophy of science. Since I have no such comprehensive view to offer, I approach the task I have set myself with humility. And also with the cowardly resolve to issue disclaimers whenever the going gets too rough."

John Earman, *Primer on Determinism* (1986)

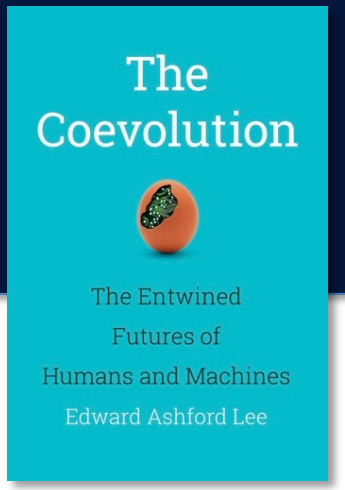
Resolution of Alternatives

The essential questions:

When, how, and why are alternatives resolved?

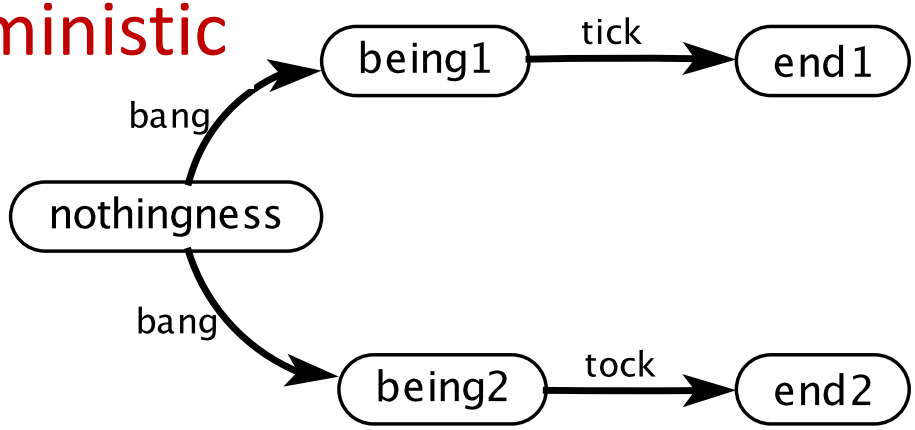
These are three different questions!

Focus on *When* Alternatives are Resolved



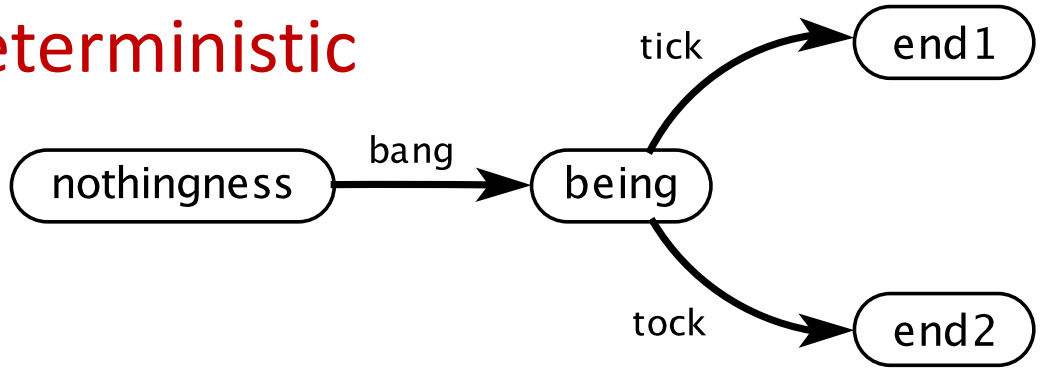
Possible tiny universes:

Deterministic

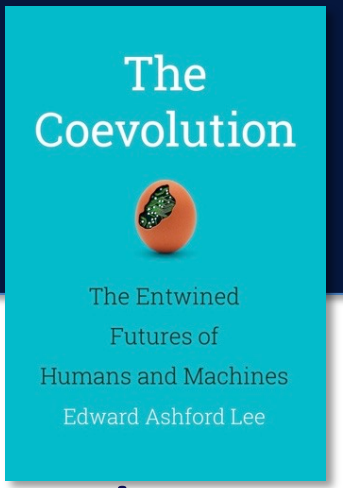


Language:
(bang, tick)
(bang, tock)

Nondeterministic



Impossibility

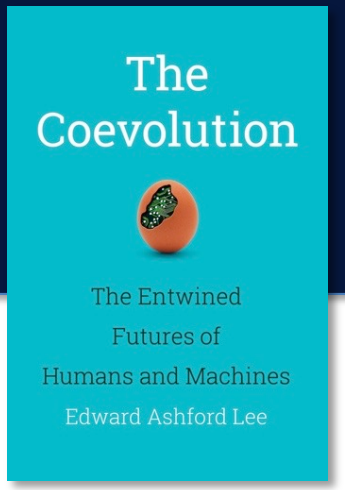


It is impossible to tell *objectively* (by observation alone) which of these scenarios is true.

This follows from Robin Milner's notion of bisimulation relations between automata.

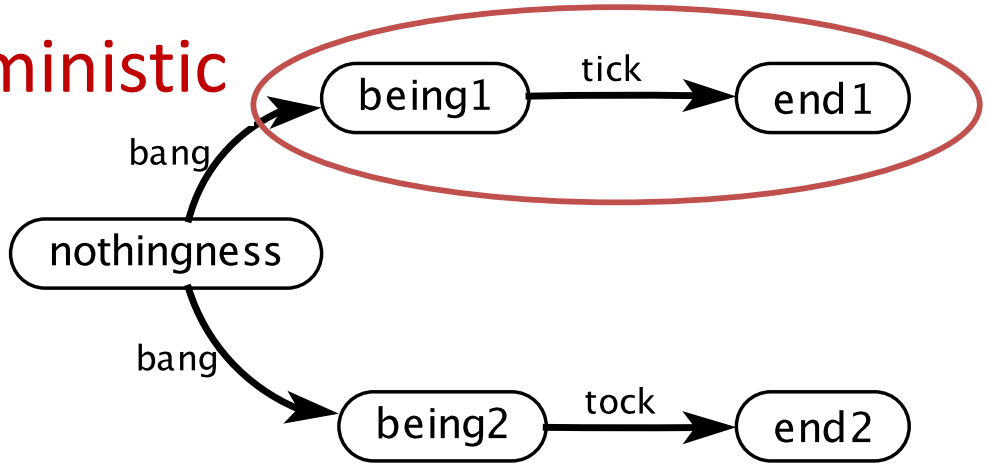
It *is* possible to tell the difference with subjective, first-person, *interaction,* but not up to 100% confidence.

Given the *Model*, however, the difference is obvious.

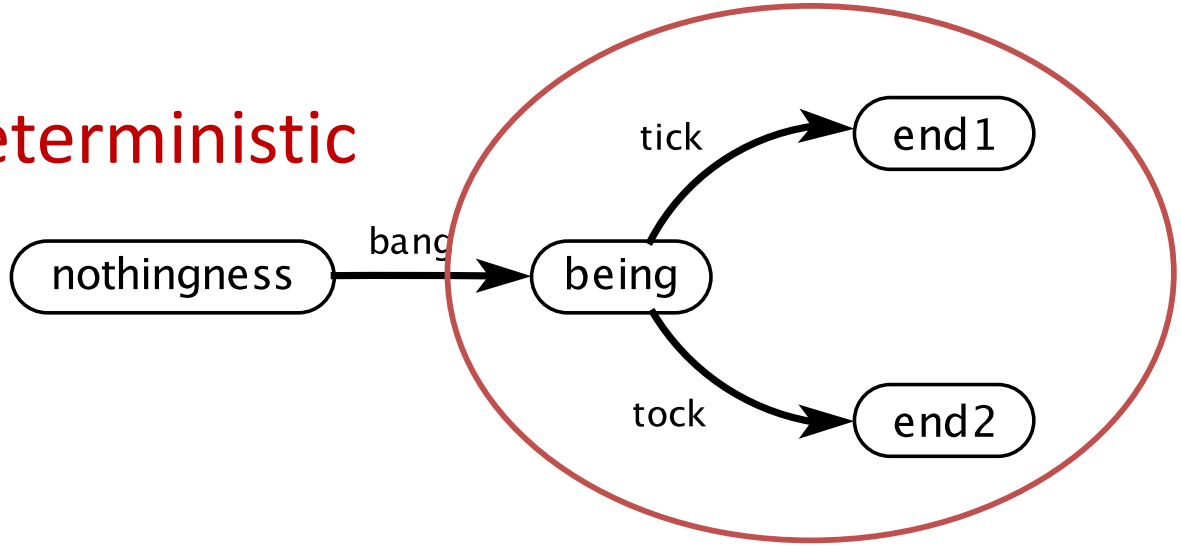


Possible tiny universes:

Deterministic



Nondeterministic



Language:
(bang, tick)
(bang, tock)

Determinism as a Property of Models

A **model** is *deterministic* if, given the initial *state* and the *inputs*, the model defines exactly one *behavior*.

Some Deterministic Models in Engineering Practice

Single-threaded imperative programs

Model

```
1  void foo(int32_t x) {
2      if (x > 1000) {
3          x = 1000;
4      }
5      if (x > 0) {
6          x = x + 1000;
7          if (x < 0) {
8              panic();
9          }
10     }
11 }
```

Instruction set architecture (ISA)

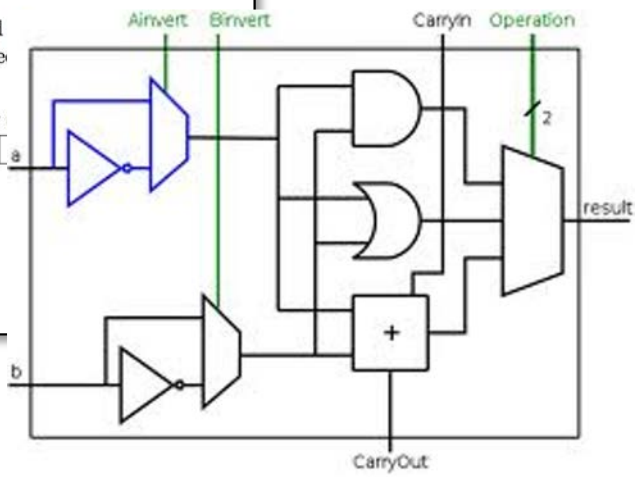
Integer Register-Register Operations

RISC-V defines several arithmetic R-type operations. All operations read as source operands and write the result into register *rd*. The *funct* field sele

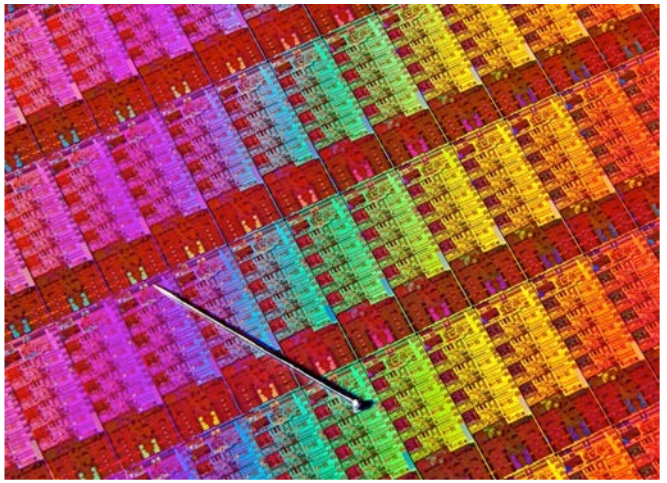
31 27	26 22	21 17	16 7
rd	rs1	rs2	funct10
5	5	5	10
dest	src1	src2	ADD/SUB/SLT/SLTU
dest	src1	src2	AND/OR/XOR
dest	src1	src2	SLL/SRL/SRA
dest	src1	src2	ADDW/SUBW
dest	src1	src2	SLLW/SRLW/SRAW

Waterman, et al., The RISC-V Instruction Set Manual, UCB/EECS-2011-62, 2011

Synchronous digital logic



Physical System



Images: Wikimedia Commons

The Value of Deterministic Models

- **Repeatability**
  - Same input, same outputs. **Testing**.


RESEARCH-ARTICLE OPEN ACCESS

Determinism

Author: Edward A. Lee Authors Info & Affiliation

ACM Transactions on Embedded Computing Systems, 34 • https://doi.org/10.1145/3453652

Some nondeterministic designs are untestable

NASA's Toyota Study (US Dept. of Transportation, 2011) found that Toyota software was “untestable.”

Possible victim of unintended acceleration

The Value of Deterministic Models

- **Repeatability**
  - Same input, same outputs. **Testing**.
- **Consensus**
  - Independent agents agree.
- **Predictability**
  - *Some* deterministic models are predictable.

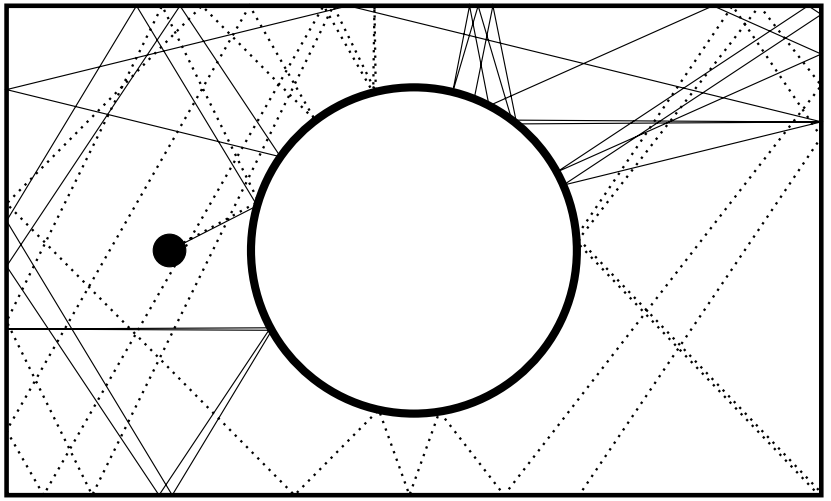

RESEARCH-ARTICLE OPEN ACCESS

Determinism

Author: Edward A. Lee Authors Info & Affiliation

ACM Transactions on Embedded Computing Systems, 34 • https://doi.org/10.1145/3453652

Determinism Does Not Imply Predictability!



Lewis and MacGregor (2006) thought experiment:

- Two spheres colliding.
- Precision of initial conditions needed to predict behavior.
- Measure positions optically.
- Find the required wavelength of light.
- A single photon of such light would have "more energy than is currently posited for the entire universe in order to resolve the initial state of the system with precision sufficient to predict its behavior after just 35 collisions."

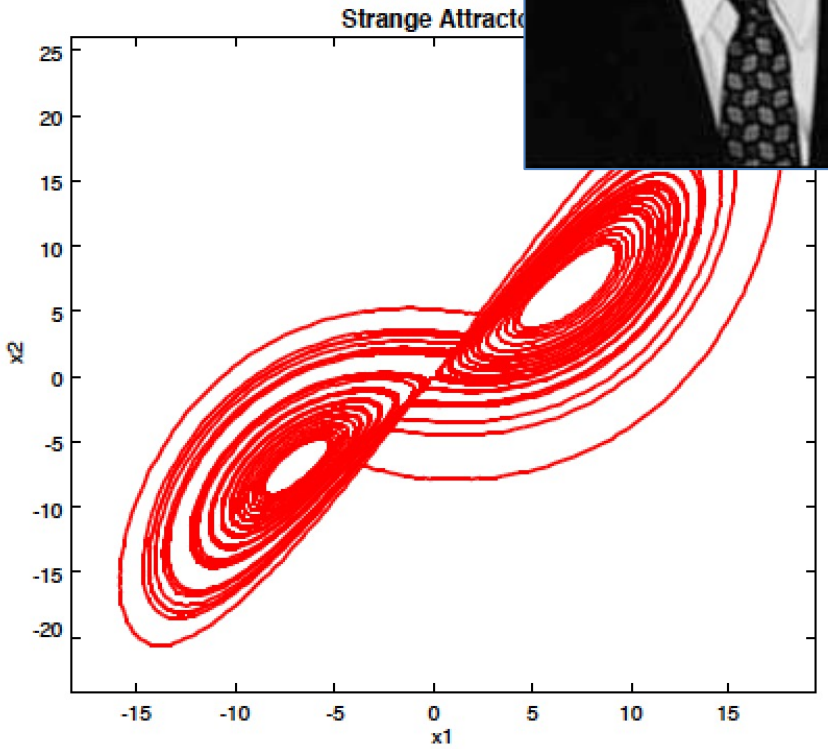
Chaos

Edward Lorenz

Lorenz attractor:

$$
\begin{aligned}
\dot{x}_1(t) &= \sigma(x_2(t) - x_1(t)) \\
\dot{x}_2(t) &= (\lambda - x_3(t))x_1(t) - x_2(t) \\
\dot{x}_3(t) &= x_1(t)x_2(t) - bx_3(t)
\end{aligned}
$$

Plot of x_1 vs. x_2:



The error in x_1 and x_2 due to numerical approximation is limited only by the stability of the system.

Chaos in Real-Time Scheduling

Deterministic real-time scheduling results in chaos.

[Thiele and Kumar, EMSOFT 2015]

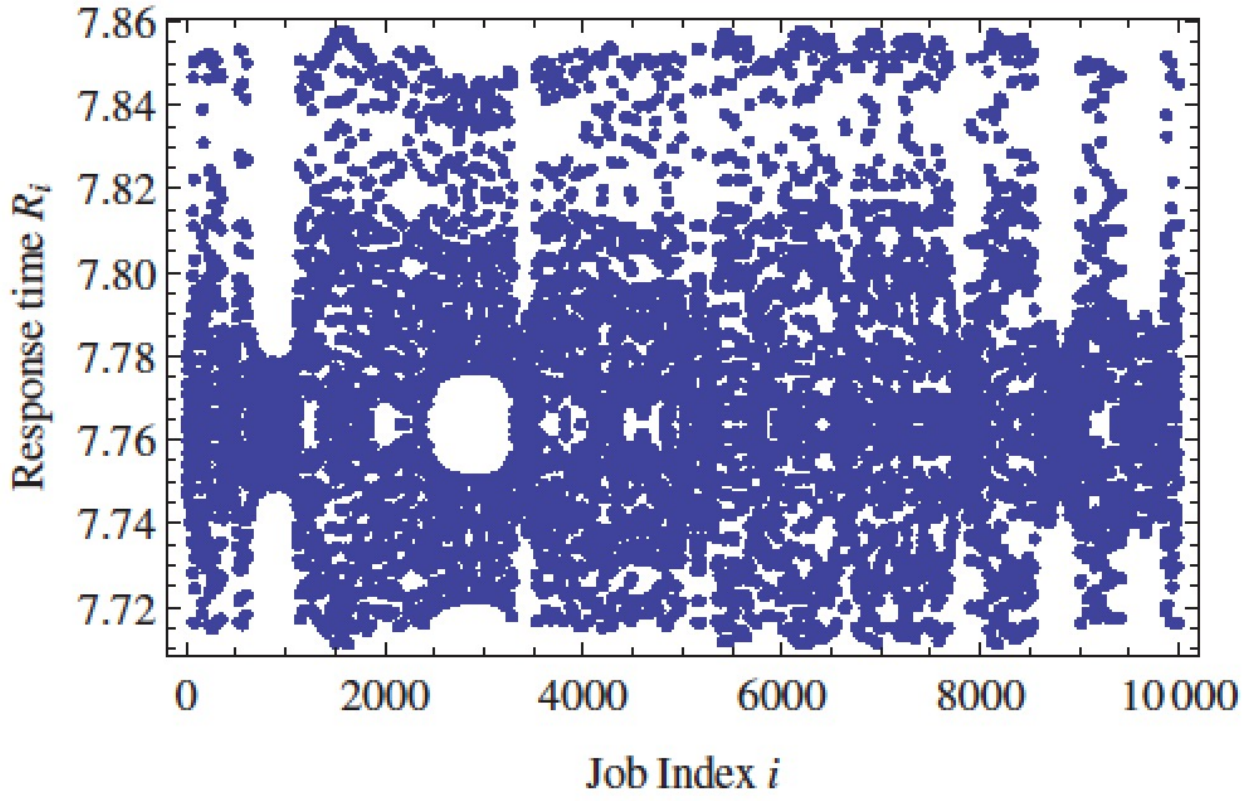


Fig. 15. Response time across jobs for the multi-resource scheduler with $R_s(i-1) = 7.76$ and $R_s(i-2) = 7.74$.

The Value of Deterministic Models


RESEARCH-ARTICLE OPEN ACCESS

Determinism

Author: Edward A. Lee Authors Info & Affiliatio

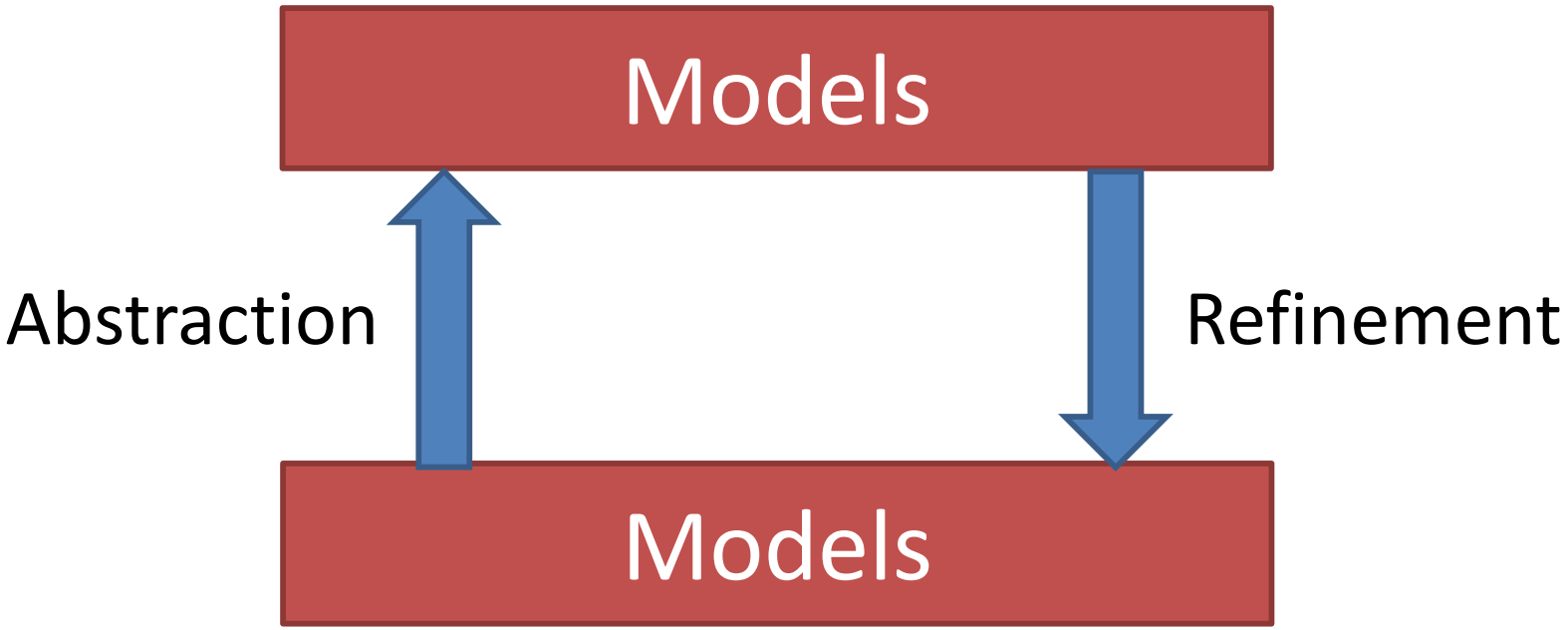
ACM Transactions on Embedded Computing Systems, 34 • https://doi.org/10.1145/3453652

- **Repeatability**
  - Same input, same outputs. **Testing**.
- **Consensus**
  - Independent agents agree.
- **Predictability**
  - *Some* deterministic models are predictable.
- **Fault Detection**
  - Correct behavior is well defined.
- **Simplicity**
  - One correct behavior for each input.
- **Unsurprising Behavior**
  - Boring is good.
- **Composability**.
  - Component behavior is clear; composition behavior too.

The Value of *Nondeterministic* Models

- **Abstraction**
  - Nondeterministic abstractions may be easier to understand.

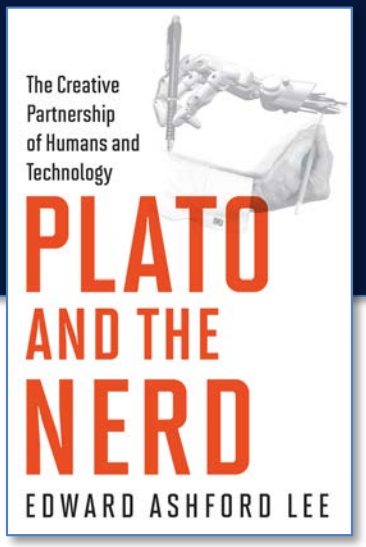
Abstraction and Refinement

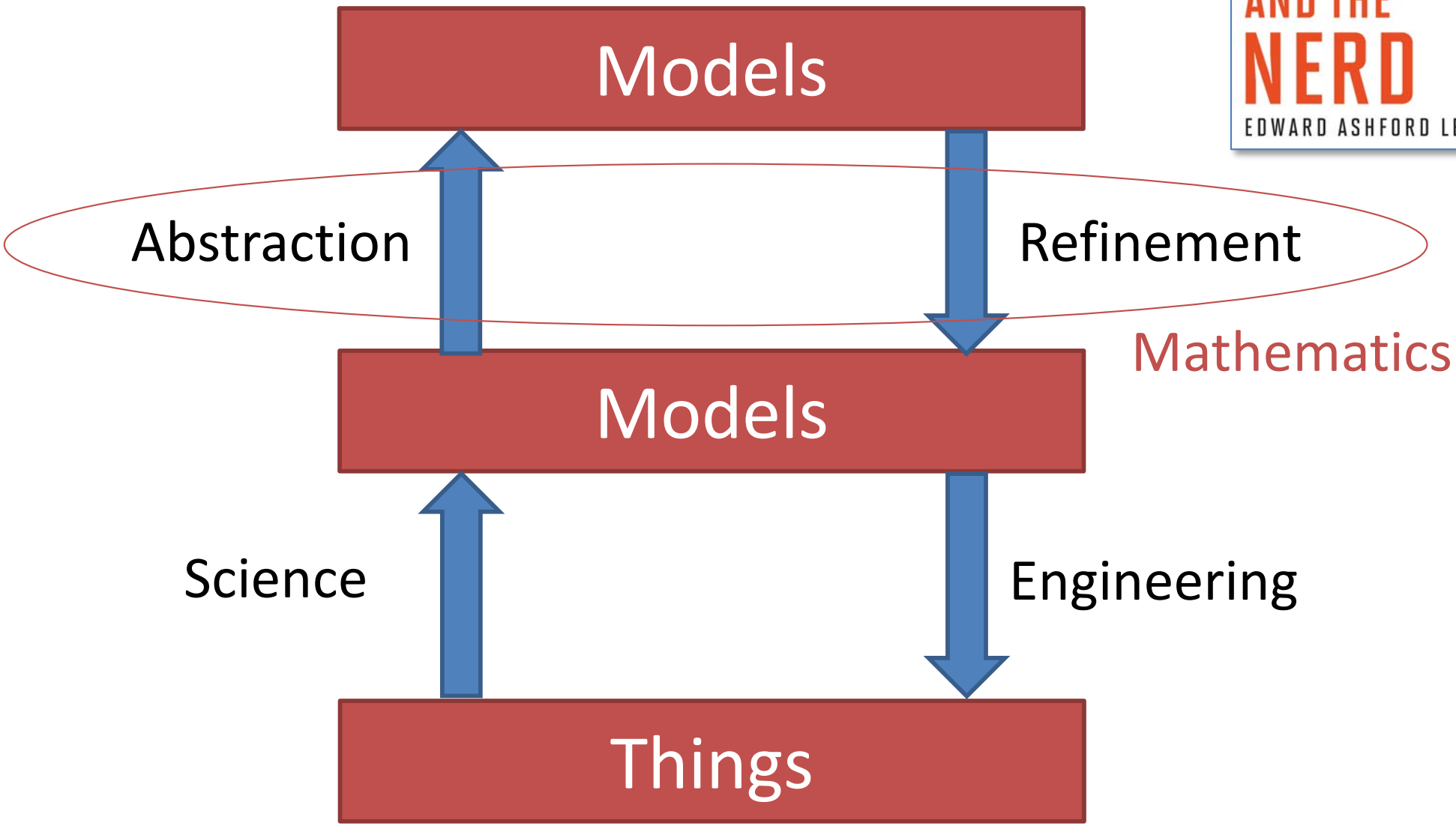


The Value of *Nondeterministic* Models

- **Abstraction**
  - Nondeterministic abstractions may be easier to understand.
- **Uncertainty (about the world)**
  - Model something not fully understood (**scientific model**)
- **Uncertainty (about the design)**
  - Deferred design decisions (**engineering model**).

Science, Engineering, and Mathematics





The Value of Models

- In *science*, the value of a *model* lies in how well its behavior matches that of the physical system.

- In *engineering*, the value of the *physical system* lies in how well its behavior matches that of the model.

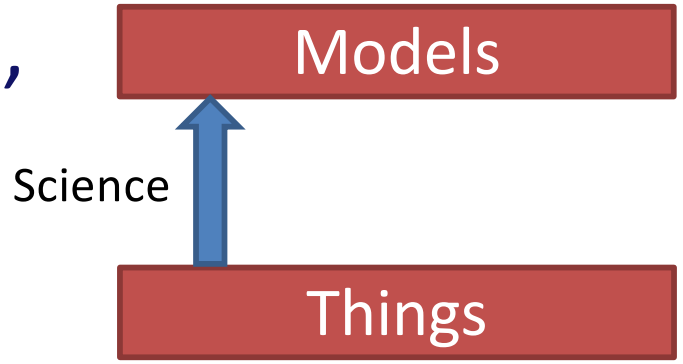
A scientist asks, "Can I make a model for this thing?"
An engineer asks, "Can I make a thing for this model?"

A Lingua Franca program is an *engineering model*, so its value depends on the ability of the physical system to match the model.

Useful Models and Useful Things

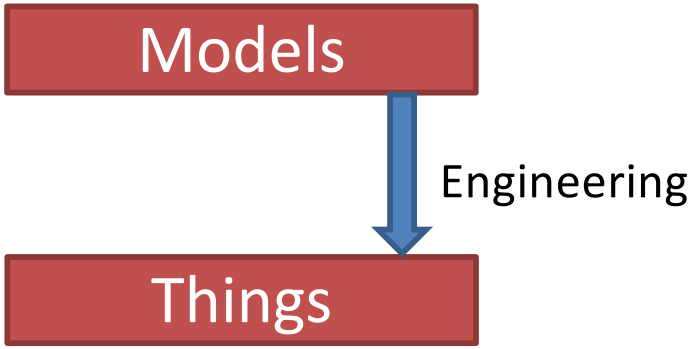
"Essentially, all models are wrong, but some are useful."

Box and Draper (1987)



"Essentially, all system implementations are wrong, but some are useful."

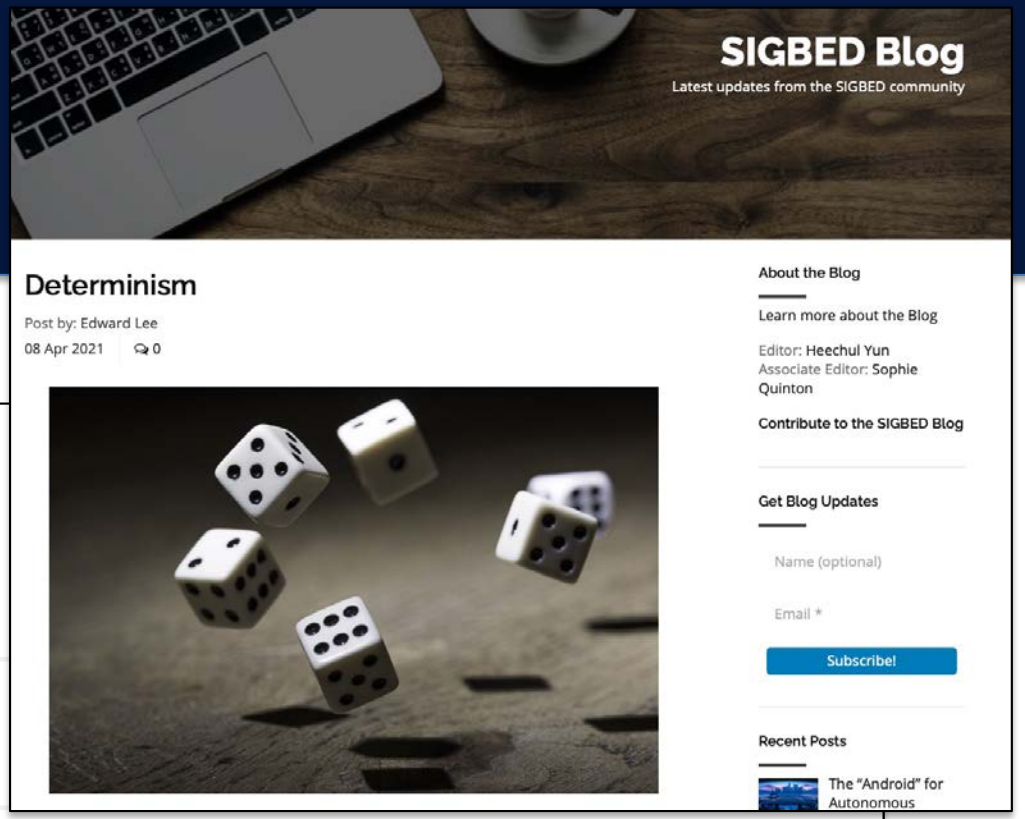
Lee and Sirjani (2018)



The Value of *Nondeterministic* Models

- **Abstraction**
  - Nondeterministic abstractions may be easier to understand.
- **Uncertainty**
  - Model something not fully understood (scientific model)
- **Deferred Design Decisions**
  - Uncertain specification (engineering model).
- **Security**
  - Unpredictability can be good.
- **Don’t Care**
  - Many behaviors are OK for the same input.
- **Surprising Behavior**
  - Boring is bad.

References



RESEARCH-ARTICLE OPEN ACCESS

Determinism

Author: Edward A. Lee Authors Info & Affiliations

ACM Transactions on Embedded Computing Systems, Volume 20, Issue 5 • July 2021 • Article No.: 38, pp 1–34 • https://doi.org/10.1145/3453652

http://ptolemy.org/~eal
eal@berkeley.edu

http://repo.lf-lang.org
Lingua Franca