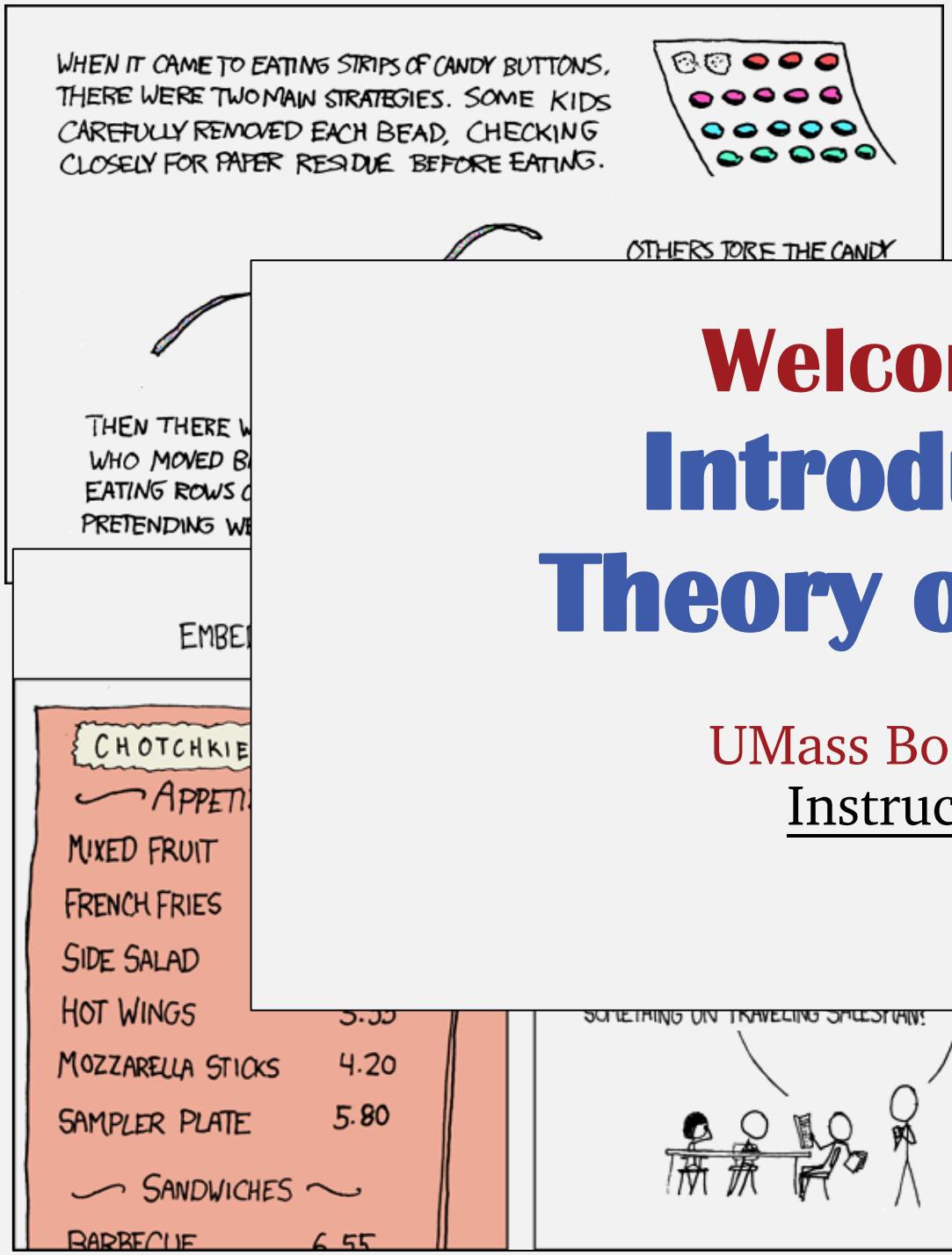
Welcome to CS420!

Introduction to the Theory of Computation

UMass Boston Computer Science
Instructor: Stephen Chang
Spring 2021



[Source: xkcd.com]

Test Poll

Lecture Logistics

- Lectures will be recorded and posted to Blackboard
- Keep audio and video off normally
- I may call on students randomly
  - This helps me to get to know each of you individually
  - Turn on audio and video at this time
  - Please be presentable
- Type questions into Zoom's chat
  - Don't use the hand raise feature
  - Please be patient since I may only monitor occasionally

What is Computer Science?

- What is a COMPUTER?
  - Many different kinds, with varying “power”

- What is SCIENCE?

Science

From Wikipedia, the free encyclopedia

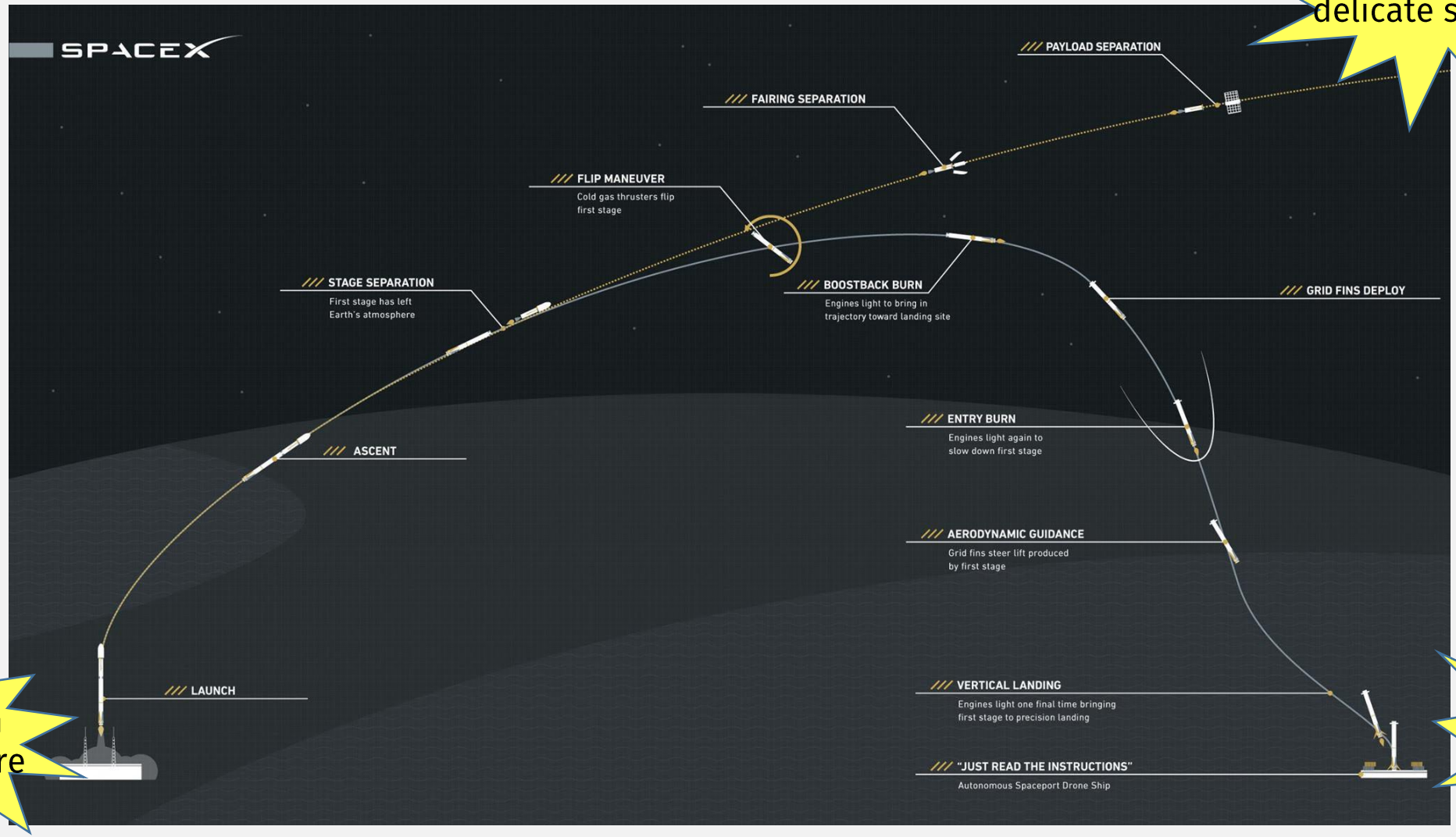
This article is about a branch of knowledge. For other uses, see Science (disambiguation).

Science (from the Latin word *scientia*, meaning "knowledge")[1] is a systematic enterprise that builds and organizes knowledge in the form of testable explanations and predictions about the universe.[2][3]

  - I.e., Science is about creating predictive **models**

In physics, models can predict …

Drop off $1b of delicate stuff here



Do 1000 ton explosion here

Land exactly here

Models predict … with varying accuracy

Some models are worthless

> We were seeing things that were
> 25-standard deviation moves
> [a 25 std dev event happens once every 100,000 **years**],
> several days in a row.

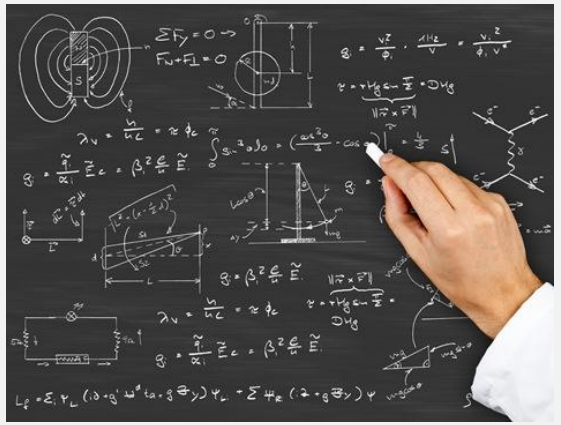
David Viniar, Goldman Sachs CFO,
August 2007 financial crisis

The theory of computation is about …

- Mathematical models of computers
- What does it mean to “model” a computer??
- Why make predictions about computers??
- What predictions about computers are possible??

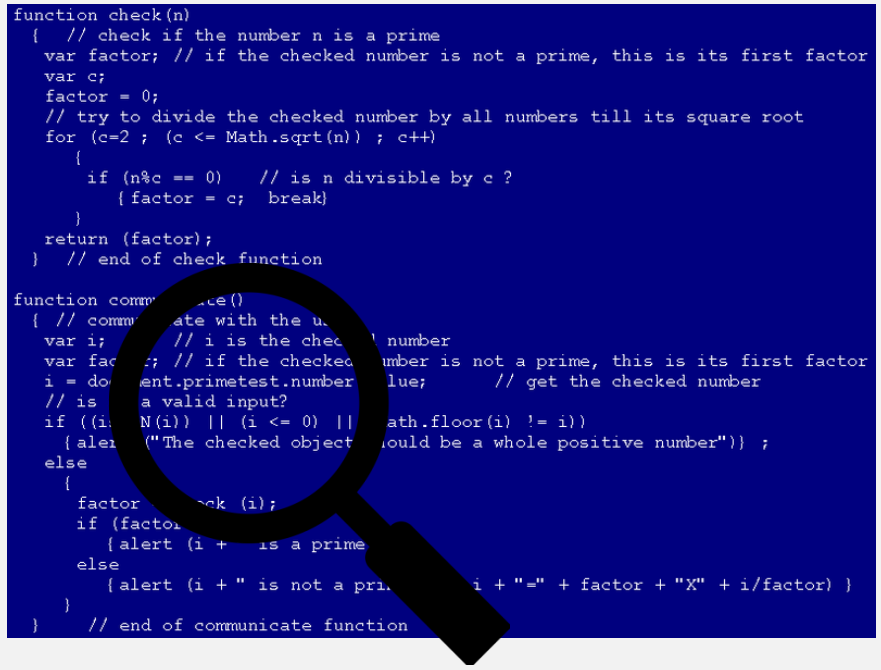
Math: The “Language” of Models

- Physics: algebra, calculus, differential eqs
- Biology: probability
- Computer Science:
  - **discrete math, set theory, mathematical logic**
  - See Chapter 0 in the textbook:
  - *Intro to the Theory of Computation*, 3rd ed, by Michael Sipser



This is (mostly) a math course!

Why make predictions about computers?

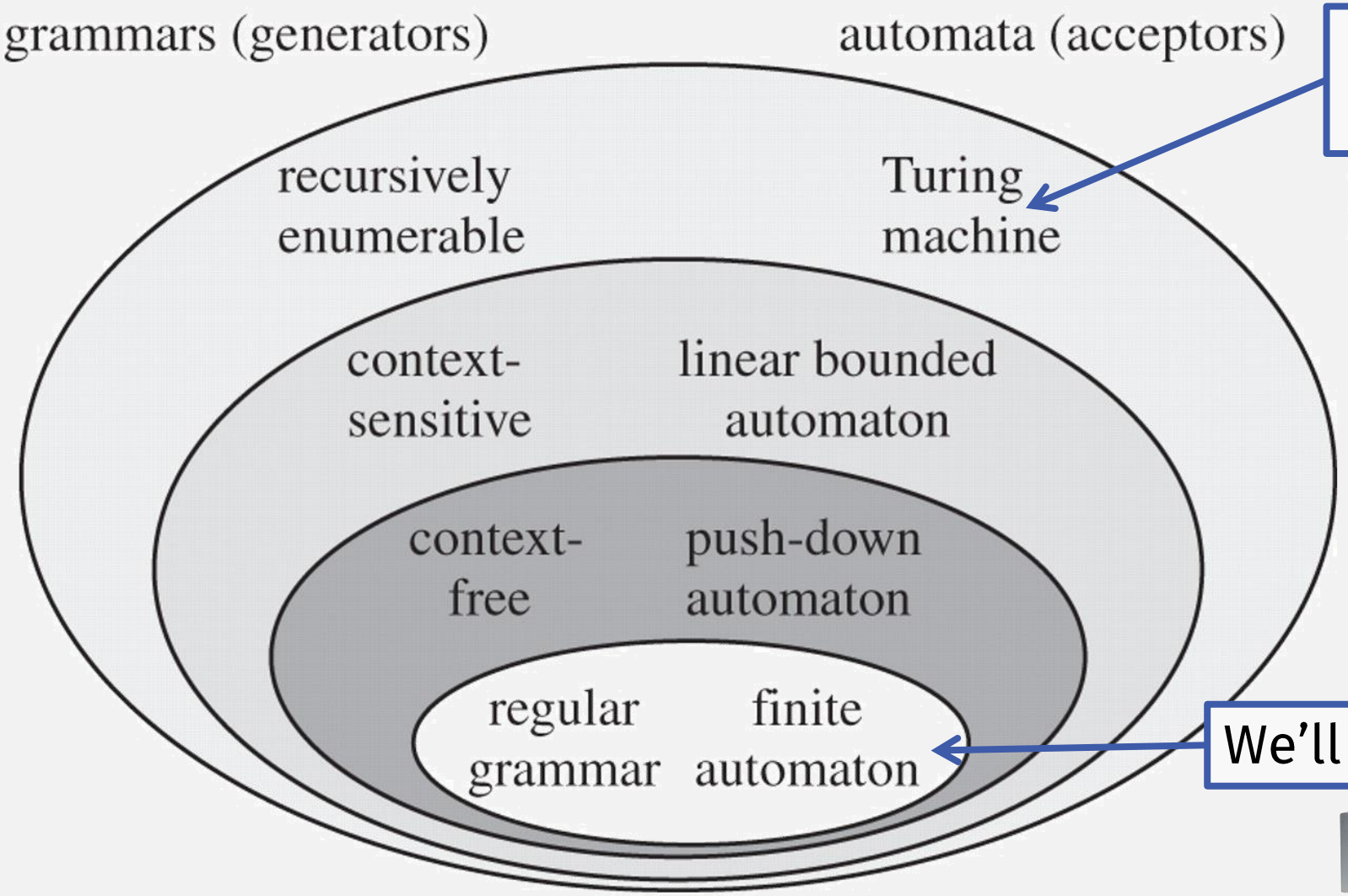


Can we make predictions about computers?

- The **Halting Lemma** says:

- And **Rice's Theorem** says:
  - "all non-trivial, semantic properties of programs are undecidable"
- Actually:
  - it depends on the computation model!

Many levels of computational power



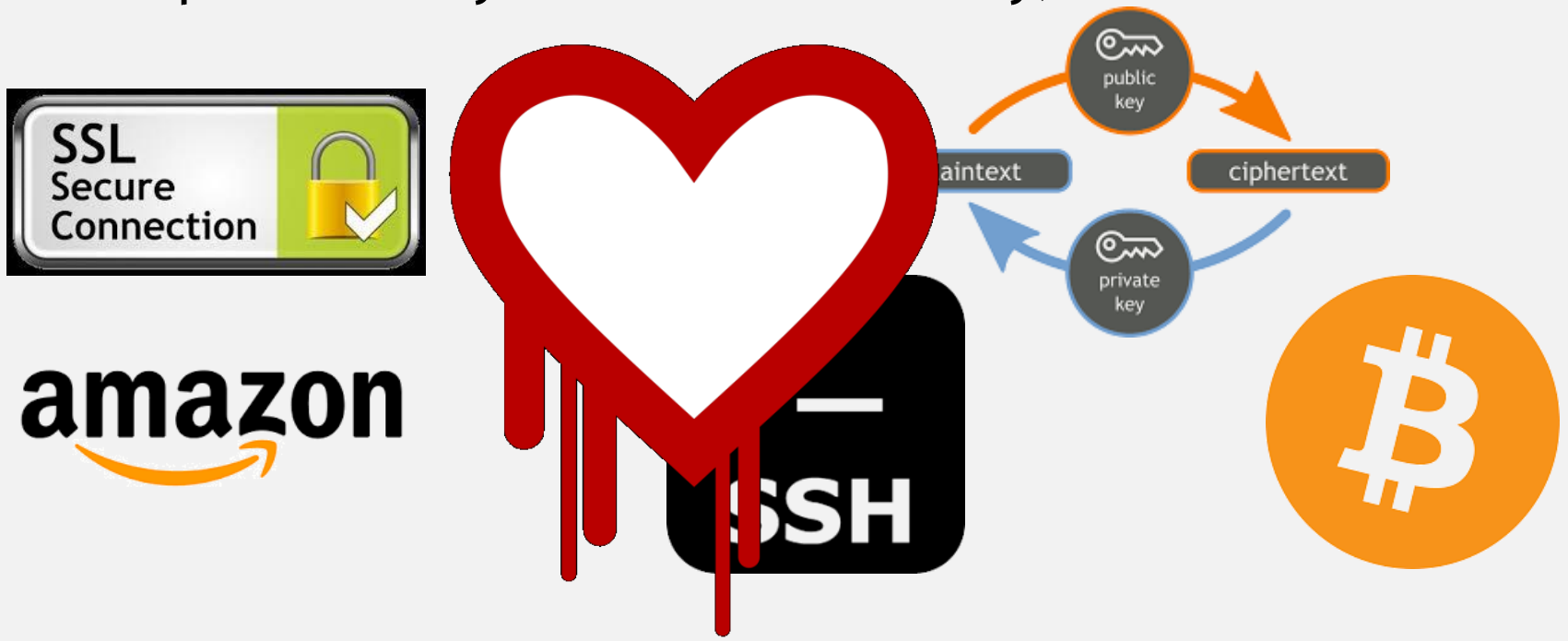
Halting Lemma, Rice's Theorem

- more complex
- more powerful
- less restricted

We'll start here

And Knowing What Computers Can't Do is Still Useful!

- In Cryptography:
  - Perfect secrecy is impossible in practice
  - But with slightly imperfect secrecy
    (i.e., a computationally bounded adversary):



LANGSEC: Language-theoretic Security

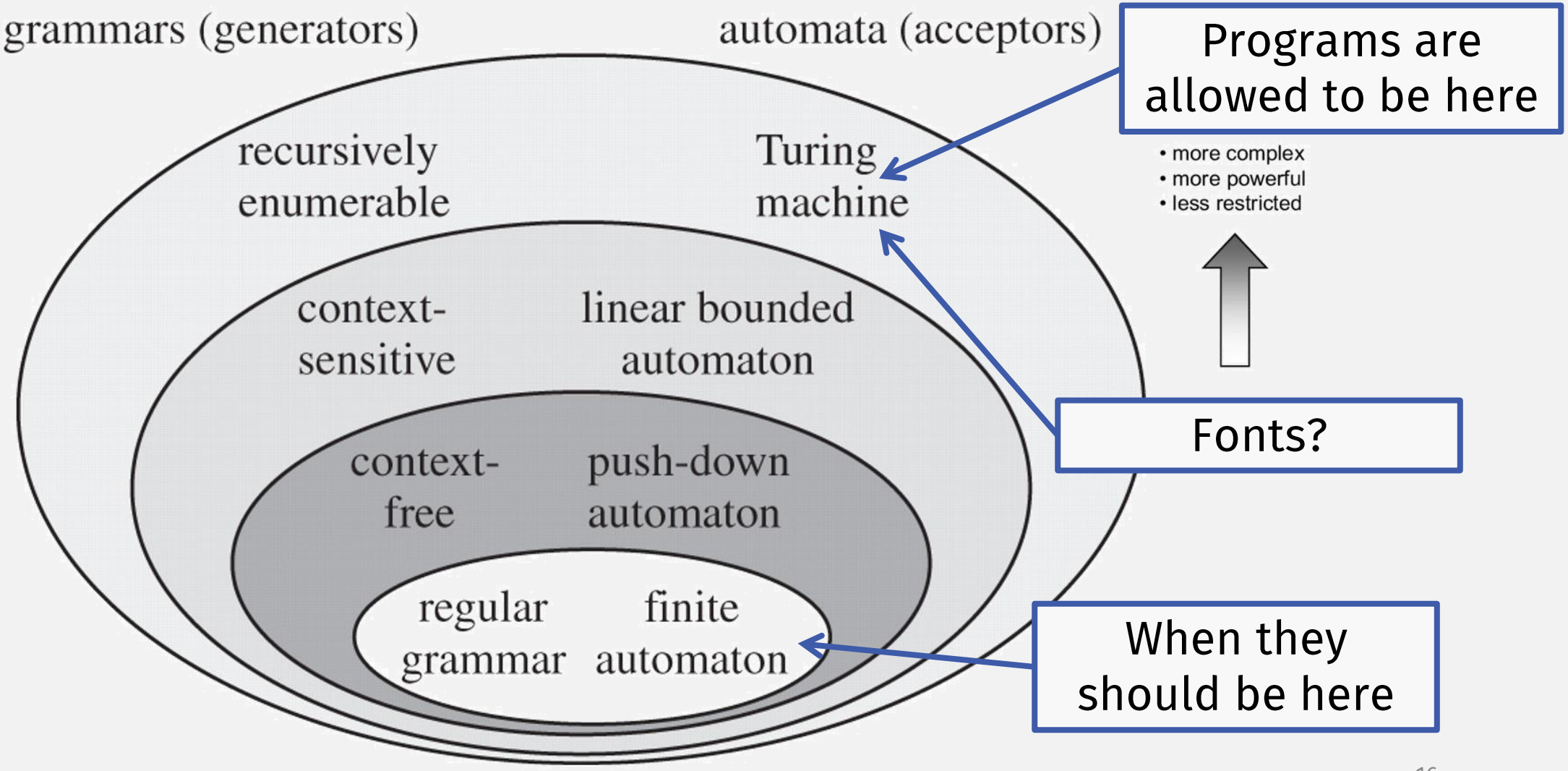
> LANGSEC is an area of research that regards
> the Internet insecurity epidemic
> as a consequence of not paying attention to
> ~~the computational power given to inputs~~

Professor Chang in CS420!!!!!111one

~~**langsec.org**~~

Prof. Chang

LANGSEC: Language-theoretic Security



What computing power should fonts have?

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & C

IN THE WILD —

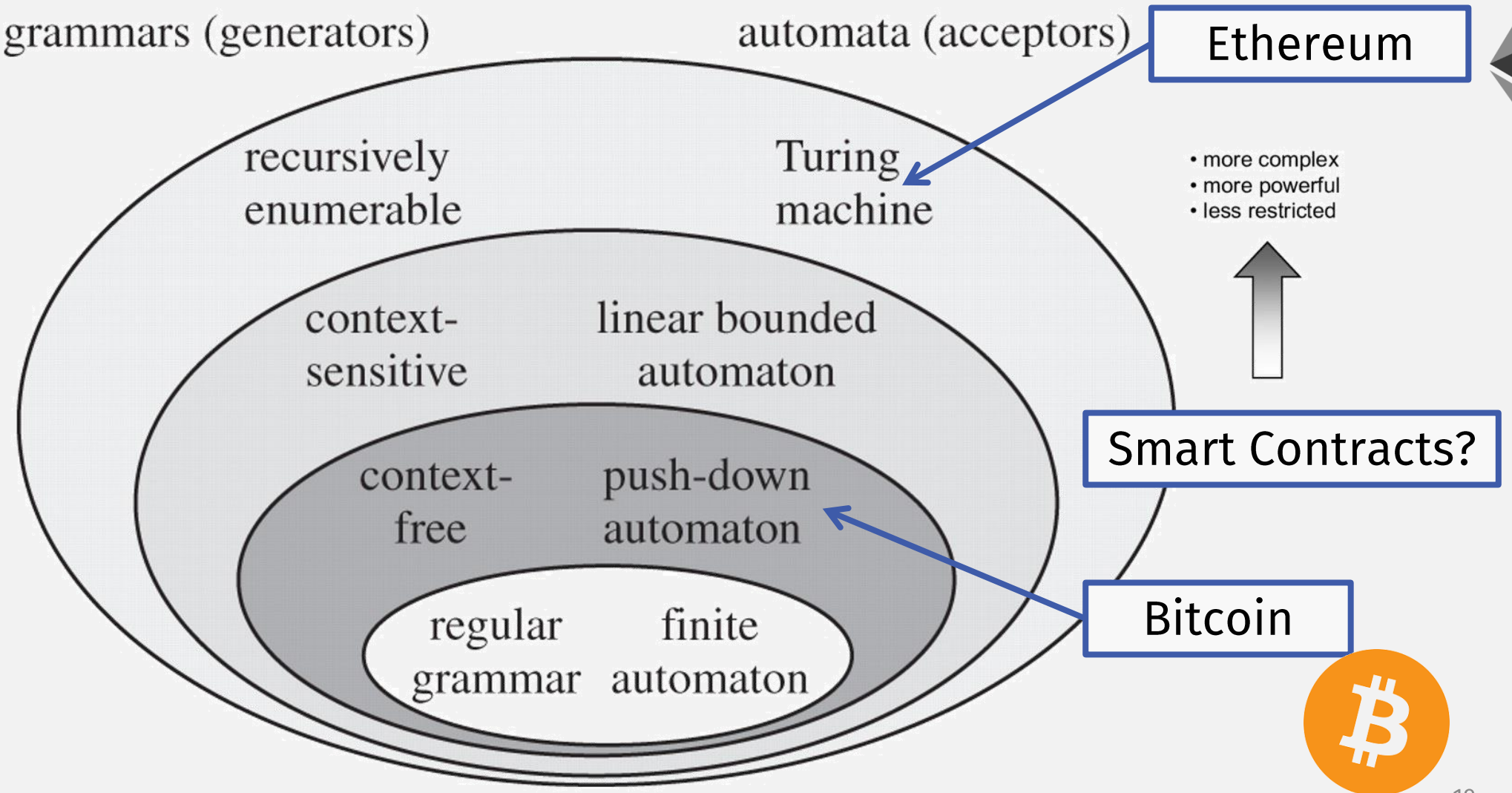
Windows code-execution zeroday is under active exploit, Microsoft warns

There's no patch available now. Here's what to do until Microsoft issues one.

DAN GOODIN - 3/23/2020, 3:40 PM

The font-parsing remote code-execution vulnerability is being used in "limited targeted attacks," against Windows 7 systems, the software maker said in an advisory published on Monday morning. The security flaw exists in the Adobe Type Manager Library, a Windows DLL file that a wide variety of apps use to manage and render fonts available from Adobe Systems. The vulnerability consists of two code-execution flaws that can be triggered by the improper handling of maliciously crafted master fonts in the Adobe Type 1 Postscript format. Attackers can exploit them by convincing a target to open a booby-trapped document or viewing it in the Windows preview pane.

LANGSEC: Language-theoretic Security



What power should smart contracts have?

The New York Times

A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency

By Nathaniel Popper

June 17, 2016

The specific mechanism the hackers used is known as a recursive call vulnerability, — essentially a malicious transaction that moves money away from the D.A.O. into a side fund in an endlessly repeating loop.

What computing power should ??? have?

NEWS

Understanding the Rosetta Flash vulnerability

14 August 2014 by Ange Albertini

To learn the answer, take CS420!!!

Android 'Master Key' Security Hole Puts 99% Of Devices At Risk Of Exploitation

Natasha Lomas @riptari / 9:20 am EDT • July 4, 2013

Comment

Check-In Quiz 1/25
(see gradescope)

Course Logistics

Course website:

https://www.cs.umb.edu/~stchang/cs420/s21/