CSE355 – Applications of Finite state machines

ASU CSE 355 – 2011.10.20

G. Fainekos

Ariane 5 - June 4th, 1996

- Video on YouTube.

Ariane 5 – The catastrophe

• Ariane 5, an unmanned rocket, was launched on 4th June 1996. The program had been running for 10 years, costing $7 billions. The rocket and its cargo itself cost $500 millions.

• The rocket exploded 37s after launching, due to software error. The error occurred when an attempt to convert a 64-bit floating point number to a signed 16-bit integer caused the number to overflow. There was no exception handler associated with the conversion so the system exception management facilities were invoked, which shut down the software.

•Interestingly, the same program functioned perfectly on Ariane 4, and was copied to Ariane 5 for that reason. What had changed, was the physical system around the software.

•Report: Ariane 501 Inquiry Board report

Lessons from Ariane 5 …

Case for model-based CPS verification:

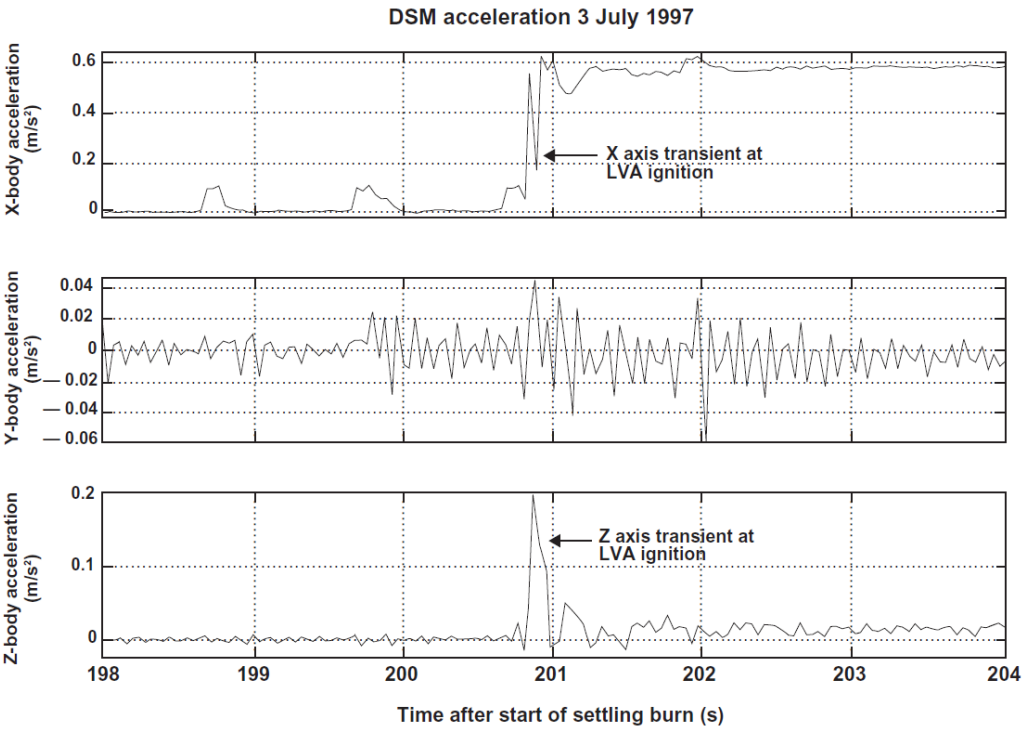
Does the embedded software "behave" correctly given the new model of the physical system?

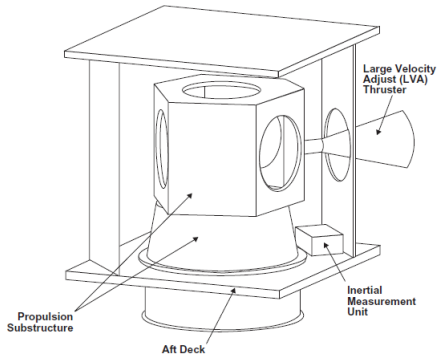
Case for model based design and automatic code generation:

Generate code for the system instead of porting code

Near Earth Asteroid Rendezvous (NEAR)*

- Dec. 20, 1998: 3 years en route to 433 Eros
- Executes a 15min main engine burn to place vehicle in orbit about the asteroid
- The software detects a transient in the lateral acceleration that exceeded the coded bounds in the software
  - the mechanical system could sustain the forces





* Hoffman, E. J.; Ebert, W. L.; Femiano, M. D.; Freeman, H. R.; Gay, C. J.; Jones, C. P.; Luers, P. J. & Palmer, J. G. The NEAR rendezvous Burn Anomaly of December 1998 Applied Physics Laboratory, Johns Hopkins University, 1999

Near Earth Asteroid Rendezvous (NEAR)

- The software shuts down the engine and uses thrusters to place NEAR in an earth-safe attitude
- After the thrusters, the software had to switch to reaction wheels for attitude control
  - Code for transition from thrusters to reaction wheels was missing!
  - The momentum was high so wheels were spinning faster than the limits set in software $\Rightarrow$ wheels were ignored in the computation
- etc etc
- Bottom line: most of the mission's fuel was wasted before earth gets control again! Mission was completed 13 months later.

Therac-25 (1985-87)

- Computerized radiation therapy with 2 modes
  - Direct electron beam: low doses of high energy for short time
  - X-rays: high energy electrons, it required 4 additional components (target, flattening filter, collimator and X-ray ion chamber) in the path of the beam
- The accidents occurred when x-ray therapy was activated without the target in place.
- 6 cases of serious injuries and deaths due to massive radiation
- Overconfidence in software to ensure safety
  - Old models had mechanical locks and old code was reused
  - System supported a multitasking environment and the software allowed concurrent access to shared data (equipment control task and operator interface task)
  - Overflow in a flag variable causing the software to bypass safety checks.

Random sampling of automobile recalls

- Volvo XC70 ELECTRICAL SYSTEM: SOFTWARE Recall – ID# 26160
  - THE DIAGNOSTIC SOFTWARE IN THE CENTRAL ELECTRONIC MODULE (CEM) MAY CAUSE A MALFUNCTION OF THE WINDSHIELD WIPER FUNCTIONALITY. IF THIS CONDITION OCCURS, THE WINDSHIELD WIPERS MAY NOT OPERATE WHEN ACTIVATED; OR IN CERTAIN CASES THE WINDSHIELD WIPERS MAY ACTIVATE WHEN NOT SWITCHED ON.
- M3 POWER TRAIN:CLUTCH ASSEMBLY Recall – ID# 35703
  - BMW IS RECALLING 2,500 MY 2008-2009 M3 PASSENGER VEHICLES WITH AN OPTIONAL DOUBLE CLUTCH TRANSMISSION. THE PROBLEM INVOLVES THE DOUBLE CLUTCH GEARBOX. IN A SITUATION OF RAPID VEHICLE DECELERATION, THE TRANSMISSION SOFTWARE MAY PERFORM A MULTISTAGE DOWNSHIFT.
- Toyota Recalls 75,000 Prius Hybrids for Software Glitch
  - Toyota Motor Sales announced on October 13th that it will carry out a voluntary recall of about 75,000 Prius hybrids sold in the United States due to a software problem. Certain 2004 and early 2005 model year Priuses could enter a "fail-safe" mode that shuts down the engine, allowing only limited operation using the electric motor. The problem, caused by a software error in the Electronic Control Module (ECM) system, triggers up to five warning lights while shutting down the engine.

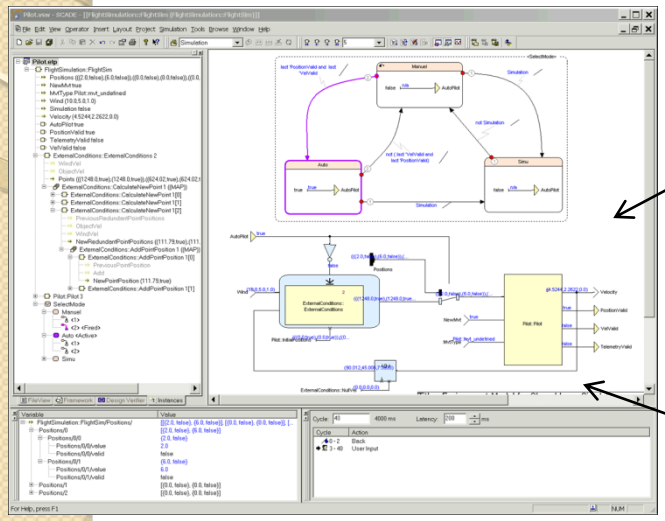
Random sampling of recalls

- 2005-2009 Mercedes SLK-Class NHTSA Campaign Number: 08V303000
  - A software calibration number (SCN) coding received on the affected vehicles during a recent workshop visit was incorrect. Depending on the model year and model affected, the results of an incorrect SCN coding can affect a number of vehicle safety and emission functions including the following types of functions: (1) the fuel gauge readings may be incorrect; (2) a stuck fuel-level sensor may not be displayed in the instrument cluster; (3) the OBD system may cause the check engine light to illuminate incorrectly; and, (4) the speedometer may be out of tolerance. In the event of a vehicle crash, the electrical fuel pump may not receive a crash signal that is required for the fuel pump to disconnect and prevent future fuel delivery as designed.

- F-350 POWER TRAIN:AUTOMATIC TRANSMISSION:CONTROL MODULE (TCM, PCM) Recall – ID# 24950
  - Model Affected 2008 FORD F-350
  - ON CERTAIN TRUCKS EQUIPPED WITH A 6.4L DIESEL ENGINE, EXCESSIVE TEMPERATURES IN THE DIESEL PARTICULATE FILTER IN THE EXHAUST SYSTEM MAY RESULT FROM EXCESS HYDROCARBONS IN THE EXHAUST.
  - LACK OF POWER OR ROUGH OPERATION, UNUSUAL NOISES FROM THE ENGINE OR EXHAUST, WHITE SMOKE FROM THE EXHAUST, AND POTENTIALLY A VISIBLE FLAME OUT THE TAILPIPE CAN OCCUR.
  - DEALERS WILL REPROGRAM THE POWER TRAIN CONTROL MODULE.

Model-based Design (MBD)

Model based design environment



Simulink
SCADE
LabView
...

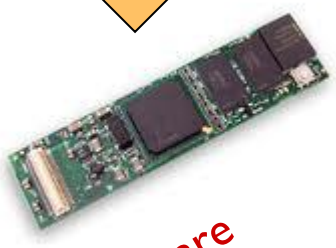
Who knows what else might appear in the future!

Modeling:
We need to know the theory and use any of the tools.

Formal Verification

Scheduling/
WCET

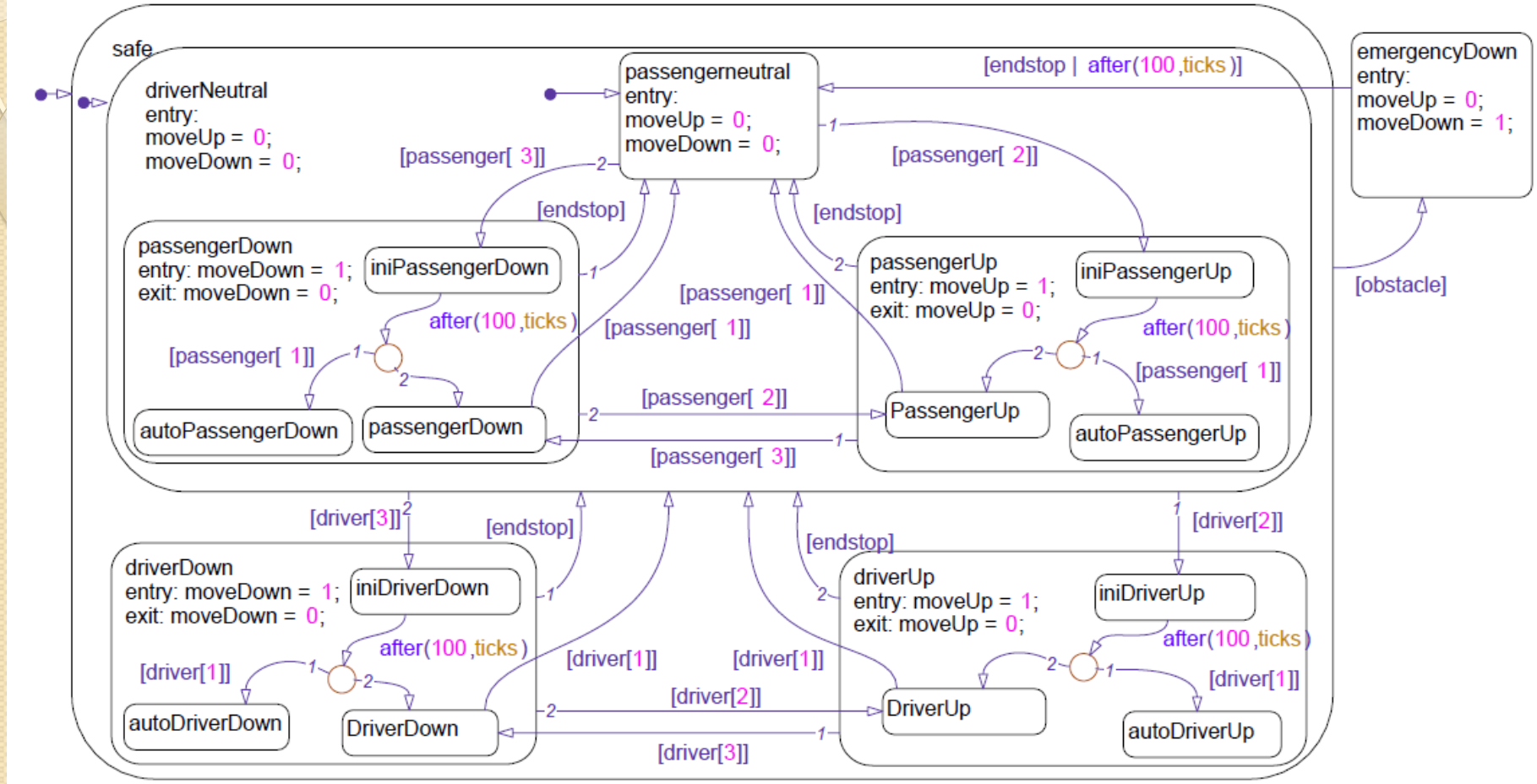
Code
Generation



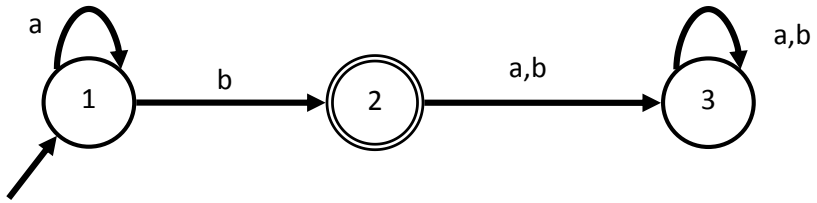
Hardware

Interfacing with
the physical world

Matlab Simulink/Stateflow model of Power window system



Compare with …

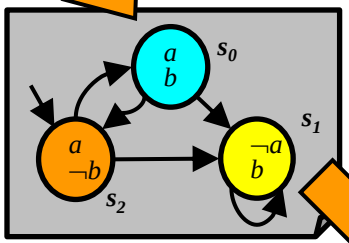


Model Checking:
Is our code correct??

```
node Val_Lim(e1 : real; Min, Max : real)
             returns (s1 : real) ;
var xmin:real, xmax : real;
let
  (xmax , xmin) = if (Max >= Min)
                  then (Max , Min)
                  else (Min , Max) ;
   s1 = if (xmax <= e1)
        then xmax
        else (if (e1 > xmin)
              then e1
              else xmin)
tel.
```

Extract model

Formalize Specification



$A[Ga \Rightarrow (Xb \vee \neg a)]$

Model Checker

YES
Witness

NO
Counter Example

Toy Model Checking: Model checking with regular languages

- Both the specification A and the system B can be viewed as languages
- The language for the specification contains all the behaviors that are considered correct

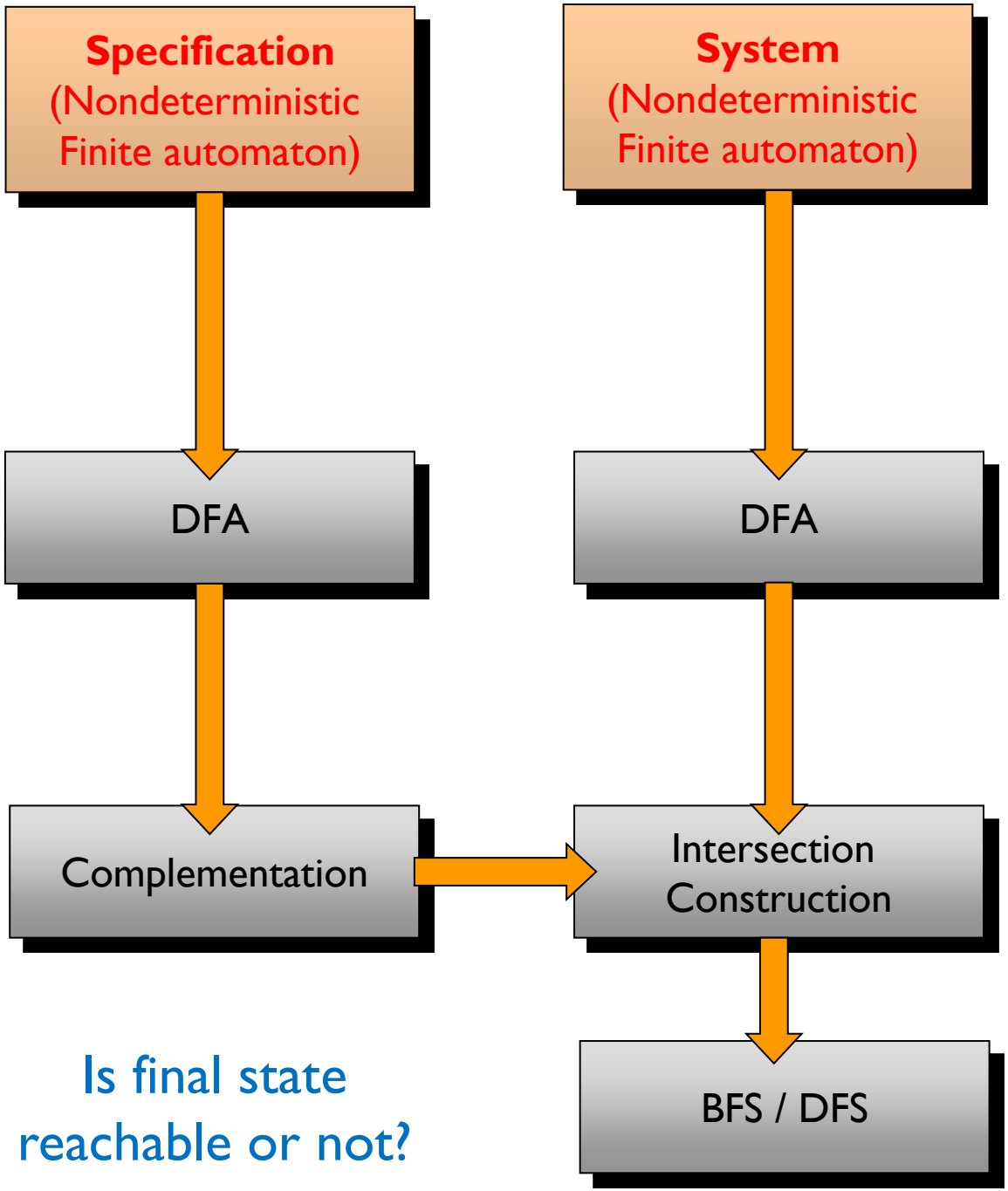
Toy Model Checking: Model checking with regular languages

- Trace containment can be turned into emptiness checking
  - "Negate" the specification, i.e., complement the specification automaton:

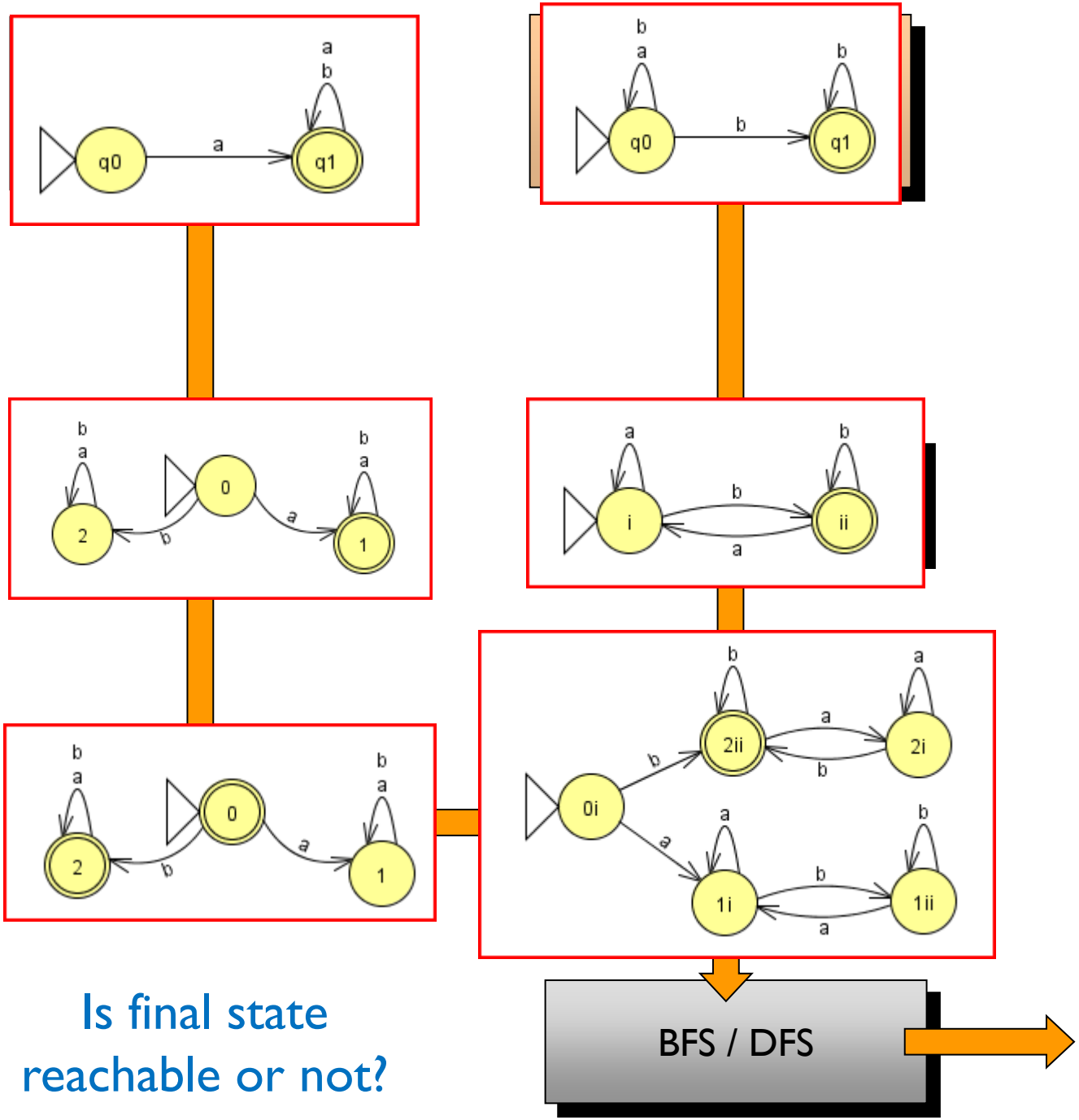
$$L(A') = \overline{L(A)}$$

  - Subset corresponds to empty intersection:

$$L(B) \subseteq L(A) \Leftrightarrow L(B) \cap \overline{L(A)} = \emptyset$$



Is final state reachable or not?


q0
a
q1
a
b
b
a
q0
b
q1
b
2
0
1
b
a
b
a
a
b
i
ii
b
a
b
a
2
0
1
b
a
b
a
a
b
0i
2ii
2i
1i
1ii
BFS / DFS
Is final state reachable or not?
String b

Companies & Laboratories

- NEC through NEC Research Labs
  - Systems Analysis & Verification Group (http://www.nec-labs.com/research/system/systems_SAV-website/index.php)
- Microsoft through Microsoft Research
  - Foundations of Software Engineering (http://research.microsoft.com/en-us/groups/foundations/)
  - Software Reliability Research (http://research.microsoft.com/en-us/groups/srr/)
  - More groups browse: http://research.microsoft.com/apps/dp/gr/groups.aspx#p=1&ps=36&so=1&sb=&fr=&to=&fd=&td=&rt=&f=&a=&pn=&pa=&pd=
- NASA JPL
  - Laboratory for Reliable Software (http://eis.jpl.nasa.gov/lars/)

Companies & Laboratories

- National Institute of Aerospace (NIA)
  - Formal Methods research program (http://www.nianet.org/resources/Research/Computational-Science/Formal-Methods.aspx)
- IBM
  - Computer Science Principles and Methodologies Group (http://www.almaden.ibm.com/cs/disciplines/pm/)
- Rockwell Collins
  - Automated Analysis (Advanced Technology Center) (http://www.rockwellcollins.com/about/innovation/atc/index.html)
- and many more (HP labs, ATT Labs, PARC etc)