Formal Languages and Specs

Neil Ernst based on V Gervasi and D Damian

Validation and Verification

- Validation criteria:
  - Discover and understand all domain properties
  - Discover and understand all requirements
- Verification criteria:
  - The program satisfies the specification
  - The **specification**, given the **domain properties**, satisfies the **requirements**

Propositional logic in formal RE specs

- A ≡ a person comes close to the door
  B ≡ the door opens
  C ≡ motion sensor is triggered
  D ≡ OPEN signal to motor

- Verification:

- Reqs: { A → B }
  Dom: { A → C, D → B }
  Spec: { C → D }
  Prove that Dom ∧ Spec → Reqs

Definition and Overview of Formal Methods

- A broad view of formal methods includes all applications of (primarily) **discrete mathematics to software engineering problems**. This application usually involves **modeling** and **analysis** where the models and analysis procedures are derived from or derived by an underlying **mathematically-precise foundation**.

- A **formal method** in software development is a method that provides formal language for describing a software artifact (for instance, specifications, designs, or source code) such that **formal proofs are possible in principle**, about properties of the artifact so expressed.

Use of Formal Methods (FM)

- Reasoning about a formal description
  The requirements problem: W,S |- R
- Verification does not eliminate the need for validation! However, the discipline of producing a formal specification can
  - result in fewer specification errors.
- When to use formal methods
  - Mostly functional requirements
  - Critical components of the system

Formal Requirements Spec

- Formal requirements specifications are specifications that have formal semantics and syntax.
- Allows a specification to be **precise, unambiguous, and verifiable**.
- Can be verified **automatically**.
- Useful in reasoning about the **relationships** between domain properties, requirements and specifications
- **Prove** properties of requirements and specs
- Good news: very useful when applied properly

Examples of FM use

- Paris metro line 14 entirely controlled by software formally developed by Matra Transport using the B abstract machine method

Formal Methods at NASA

- Given a fault, must complete **time critical activity** and **preserve space craft**.
- E.g., given detected hazardous condition, shut down all non-critical functions, ensure the antenna is pointing towards Earth, and await further commands. Maintain such a safe state for up to two weeks.
  - Cassini Requirement: If Spacecraft Safing is requested via a CDS (Command and Data Subsystem) internal request while the spacecraft is in a critical attitude, then no change is commanded to the AACS (Attitude and Articulation Control Subsystem) attitude. Otherwise, the AACS is commanded to the homebase attitude

Easterbrook: https://ntrs.nasa.gov/api/citations/19980016986/downloads/19980016986.pdf

FM at NASA (2)

- Typically these are found **informally** using inspection (often **independent team**). Challenge: **interactions**
- Formal: **SCR**. Translate prose (ambiguous) into tables showing events and triggers.
- Translate **fifteen pages** of level 3 requirements taking 1.5 person months.
- See also https://shemesh.larc.nasa.gov/fm/

Current Mode	Conditions											Next Mode
	errors in two cons. frames	bus swch'd last frame	bus switch inhibit	bus swch'd this frame	backup BC avail.	BC swch'd in last 20 sec	card reset inhibit	card reset last 10 frames	errors from mult. RTs	channel reset last frame	channel reset inhibit	
Normal	@T	-	-	F	-	-	-	-	-	-	-	switch buses
	@T	-	T	F	-	-	-	-	-	-	F	reset the
	@T	T	-	F	-	-	-	-	-	-	F	channel
	@T	-	-	-	-	-	F	F	T	T	-	reset the
	@T	-	-	-	-	-	F	F	T	F	T	card
	@T	T	-	-	-	-	-	-	F	T	-	switch R
	@T	F	T	-	-	-	-	-	F	T	-	to backu
	@T	T	-	-	-	-	-	-	F	F	T	
	@T	F	T	-	-	-	-	-	F	F	T	
	@T	-	-	-	T	F	T	-	T	T	-	switch B
	@T	-	-	-	T	F	T	-	T	F	T	to backu
	@T	-	-	-	T	F	-	T	T	T	-	
	@T	-	-	-	T	F	-	T	T	F	T	
	@T	-	-	-	T	T	T	-	T	T	-	switch
	@T	-	-	-	T	T	T	-	T	F	T	all RTs
	@T	-	-	-	T	T	-	T	T	T	-	
	@T	-	-	-	T	T	-	T	T	F	T	

Table 2: An SCR Mode transition table. Each of the central columns represents a condition, showing whether it should be true or false; '-' means "don't care"; '@T' indicates a trigger condition for the mode transition. The four columns of table 1 correspond to the last four rows of this table. The semantics of SCR require this table to represent a function, so that the disjunction of all the rows covers all possible conditions (coverage), and the conjunction of any two rows is false (disjointness).

NASA requirement

2.16.3.f) While acting as the bus controller, the C&C MDM CSCI shall set the e, c, w, indicator identified in Table 3.2.16-II for the corresponding RT to "failed" and set the failure status to "failed" for all RT's on the bus upon detection of transaction errors of selected messages to RTs whose 1553 FDIR is not inhibited in two consecutive processing frames within 100 msec of detection of the second transaction error if; a backup BC is available, the BC has been switched in the last 20 sec, the SPD card reset capability is inhibited, or the SPD card has been reset in the last 10 major (10 sec) frames, and either:

1. the transaction errors are from multiple RTs, the current channel has been reset within the last major frame, or
2. the transaction errors are from multiple RT's, the bus channel's reset capability is inhibited, and the current channel has not been reset within the last major frame.

[1] S. M. Easterbrook, R. R. Lutz, R. Covington, J. Kelly, Y. Ampo, and D. Hamilton, "Experiences using lightweight formal methods for requirements modeling," *TOSE*, vol. 24, pp. 4-14, 1998.

Verific

Cassini Requirement: If Spacecraft Safing is requested via a CDS (Command and Data Subsystem) internal request while the spacecraft is in a critical attitude, then no change is commanded to the AACS (Attitude and Articulation Control Subsystem) attitude. Otherwise, the AACS is commanded to the homebase attitude.

```
saf: THEORY
% Example is excerpted from saf theory.
% Spacecraft safing commands the AACS to homebase mode, thereby
% stopping delta-v's and desat's.
BEGIN

aacs_mode:   TYPE = {homebase, detumble}
attitude:    TYPE

cds_internal_request:   VAR bool
critical_attitude:    VAR bool
prev_aacs_mode:     VAR aacs_mode

aacs_stop_fnc (critical_attitude, cds_internal_request, prev_aacs_mode):
         aacs_mode =
         IF critical_attitude
           THEN IF cds_internal_request
                THEN prev_aacs_mode
                ELSE homebase
                ENDIF
           ELSE homebases
         ENDIF
```

```
aacs_safing_req_met_1:  LEMMA
       (critical_attitude AND cds_internal_request)
       OR (aacs_stop_fnc (critical_attitude, cds_internal_request,
          prev_aacs_mode) = homebase)

END saf
```

Outcomes

- 11 undocumented assumptions
- 10 boundary cases
- 9 traceability problems
- 6 terminology problems
- 1 logic error (pre-emptive service scheduling)

Model checking at AWS

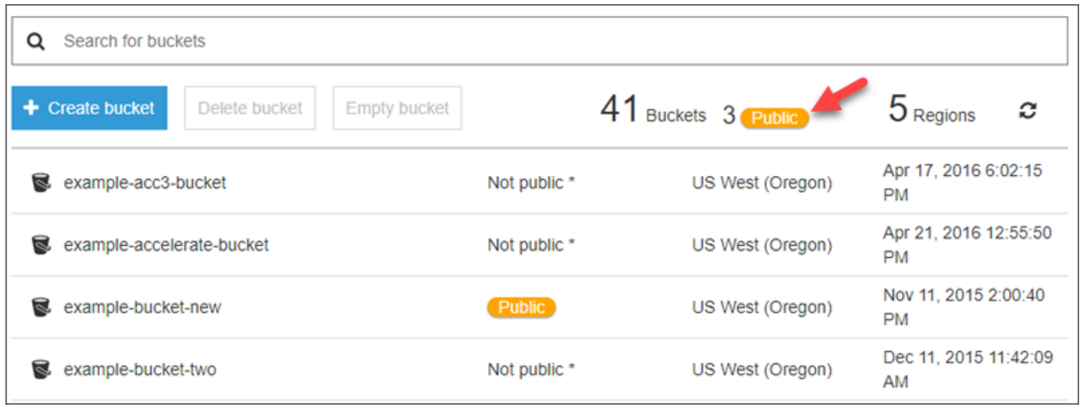
- New Key-Value store ShardStore, 40kLOC Rust code
- Validate: functional correctness of API-level calls, crash consistency of on-disk data structures, and concurrent correctness of API calls and background maintenance tasks
- Define a twin that mocks the actual object API written in Rust (rather than Alloy etc)
- Example: check that concurrent executions of ShardStore are **linearizable** with respect to the sequential reference models.
  - Use the Loom stateless model checker for Rust

.

https://assets.amazon.science/77/5e/4a7c238f4ce890efdc325df83263/using-lightweight-formal-methods-to-validate-a-key-value-storage-node-in-amazon-s3-2.pdf

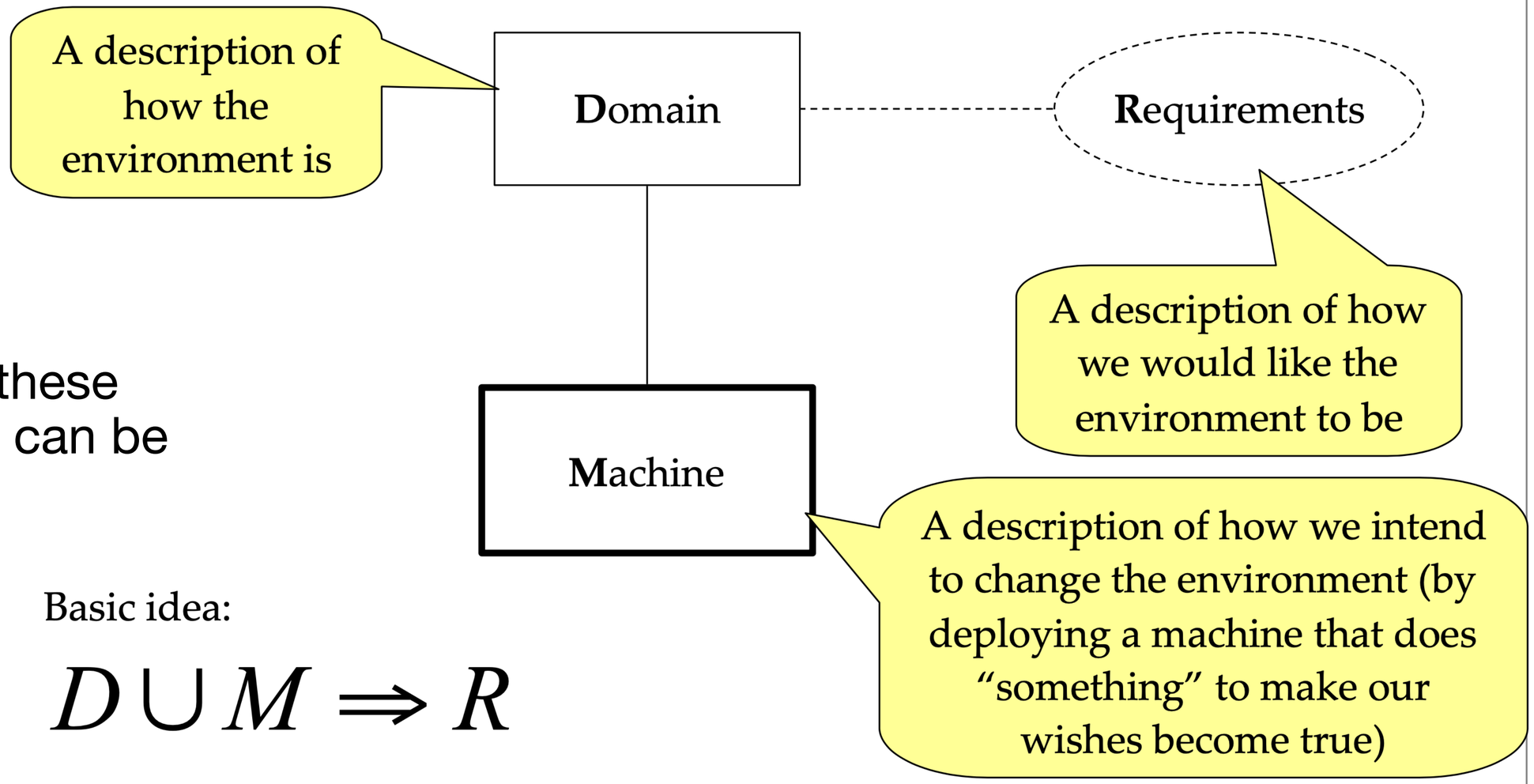
Theorem Proving at AWS

- Generate a proof to verify correctness of the system
- E.g., identity and access management: ensure no one can access a resource not on the IAM list
- (Resource = “arn:aws:s3:::test-bucket”) $\wedge$ (Principal $\neq$ 11112222333)
- Use Zelkova and SMT language



https://aws.amazon.com/blogs/security/protect-sensitive-data-in-the-cloud-with-automated-reasoning-zelkova/

The role of FMs in RE



- All or some of these yellow callouts can be formalized

Basic idea:

$$D \cup M \Rightarrow R$$

When to Apply FMs

- **After the fact**: at the end of development to aid testing and cert.
- **Parallel**: while writing code, to verify code/design/requirements.
- **Integrated**: instead of writing code, write specs and generate code.
- **Lightweight**: during requirements specification to increase quality.

An Example: Sliding Doors

- Design and implement the software for a sliding door controller (SDC) that we want to install in our restaurant (we specialize in stork soup)
- When someone comes close to the door, the door should open automatically
- Etc., e.g.: It should close after that person has entered the restaurant

Sliding doors

Requirements
When a person comes close to the door, the door should open

Specification
When the motion sensor is triggered, the system (SDC) should send the OPEN signal to the motor

Domain
- My restaurant has a motor-controlled door
- A motion sensor is installed above the door
- Motion sensors are triggered by people coming close
- A motor-controlled door opens when the motor receives the OPEN signal

A ≡ a person comes close to the door

B ≡ the door opens

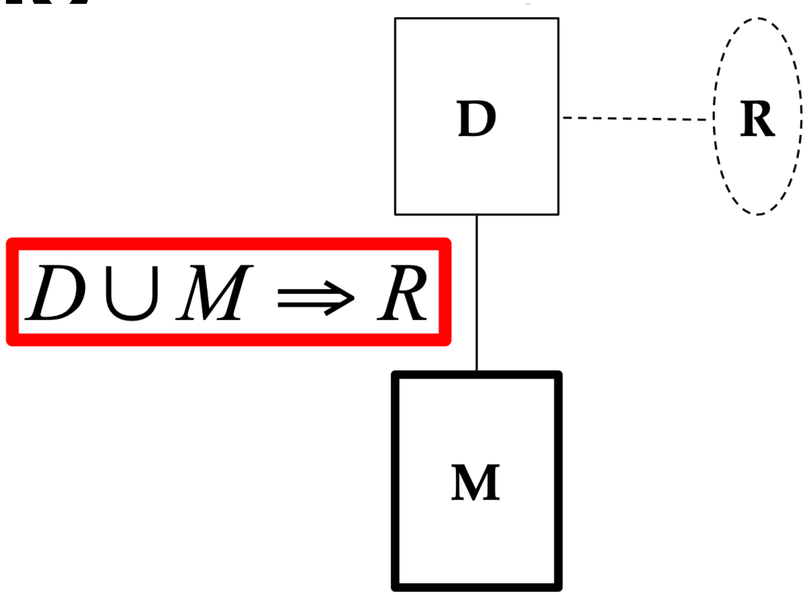
C ≡ motion sensor is triggered

D ≡ OPEN signal to motor

Formalize in Propositional Logic

The **specification**, given the **domain properties**, satisfies the **requirements**

Reqs: { A → B }
Dom: { A → C, D → B }
Spec: { C → D }
Prove that Dom ∧ Spec → Reqs



A ≡ a person comes close to the door
B ≡ the door opens
C ≡ motion sensor is triggered
D ≡ OPEN signal to motor

Types of Formal Specifications

- Property-oriented languages
  - System is described by a set of axiomatic properties
- Model-oriented languages
  - System is described by a **state**, and **operations**
  - An **operation** is a function which maps the value of the state and the value of input parameters to a new state

Automated Verification

- One major benefit for formal methods is automated verification.
- Two major categories of Verification that use Formal Methods:
  - Theorem proving
  - Model checking

Theorem Provers and Refuters

- Coq and Alloy are two well known examples
  - Prove Eve can never login: http://alloytools.org/models/simple-webattack.html
  - See also Hillel Wayne's writing: https://www.hillelwayne.com/post/alloydocs/

Model oriented languages

- The easiest way to consider a model-oriented language is as a state machine
- When the system is in a certain state, and is given a particular input, it will turn into another state
- Properties of the system are usually given using a temporal logic
- Want to verify that the model always holds the properties true

Alloy Example

See also https://www.hillelwayne.com/post/formally-modeling-migrations/

Challenges applying formal specification methods

- Limited scope (to functional requirements)
- Isolation from other software products and processes in organizations
- Cost (require high expertise in formal systems and mathematical logic)

Examples of well known formal methods and languages

- Language Z
- Communicating sequential processes (CSP)
- Vienna Development Method (VDM)
- Larch
- Formal development methodology (FDM)
- Software Cost Reduction (SCR)

Intermission

Formal verification

Prove correctness of a system using proof techniques and mathematical models

- Theorem Proving (e.g. Coq)
- Program derivation
- Formal type-checking
- Model checking
- …
- Widely used in hardware and real-time systems.

Motivation

- Problem
  - Want to check if system execution can guarantee **important properties** without **extensive** testing
- Solution
  - “**Query language**” to ask questions about execution
  - Tool which answers such queries

Overview

1. System
   - Statecharts
   - Source code
2. Properties
   - Safety
   - Liveness
   - Fairness
3. “Query language”
   - Computation Tree Logic (CTL)
4. Tool
   - Model Checker

Execution Properties

Safety

"Something bad will not happen" e.g. a null variable will never be referenced

Liveness

"Something good will happen" E.g. eventually the spinning rainbow will finish spinning

Fairness

Regardless of other properties, something good will happen.

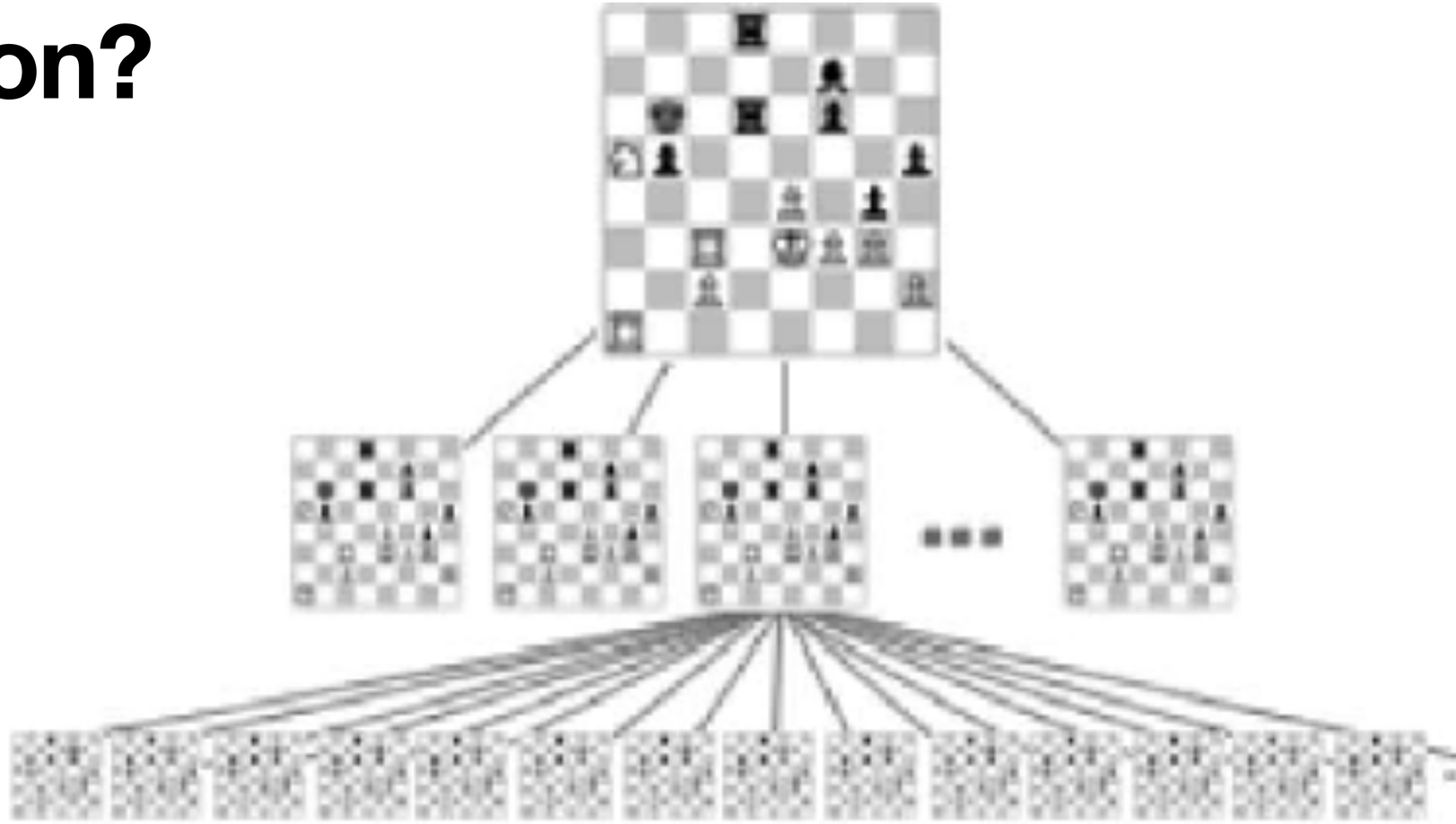
e.g. if I wait long enough, an elevator will arrive on my floor, regardless of when I arrive

Safety Requirements

- How safe should something be?
  - **Cars**: deaths per 100M miles driven? Per 100k people?
  - 1.10 fatalities per 100M miles*
  - Better than any human? All humans? Lowest cost?

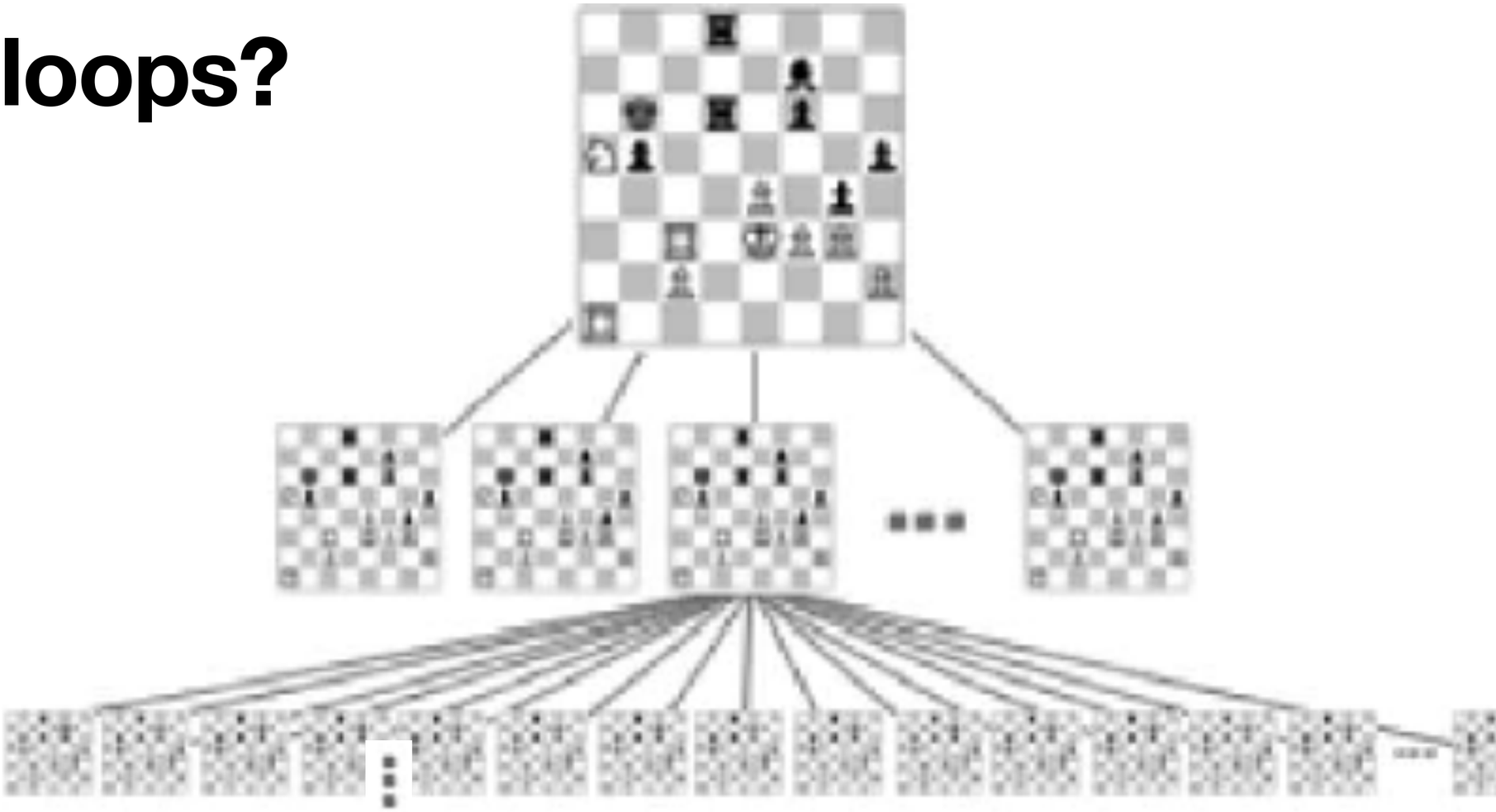
Data from https://course.ece.cmu.edu/~ece642/

What is execution?



“A tree structure in which the future is not determined; there are different paths in the future, any one of which might be an actual path that is realized”

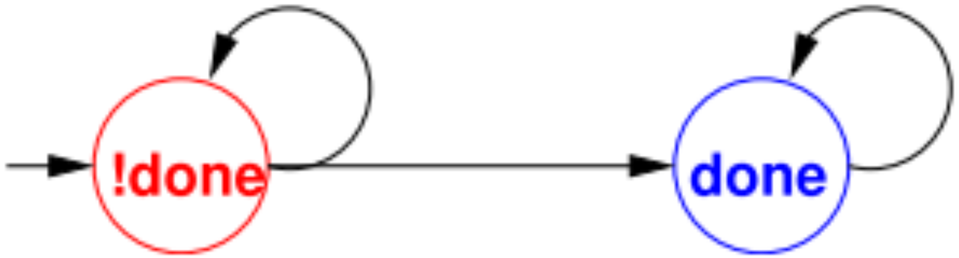
What about loops?

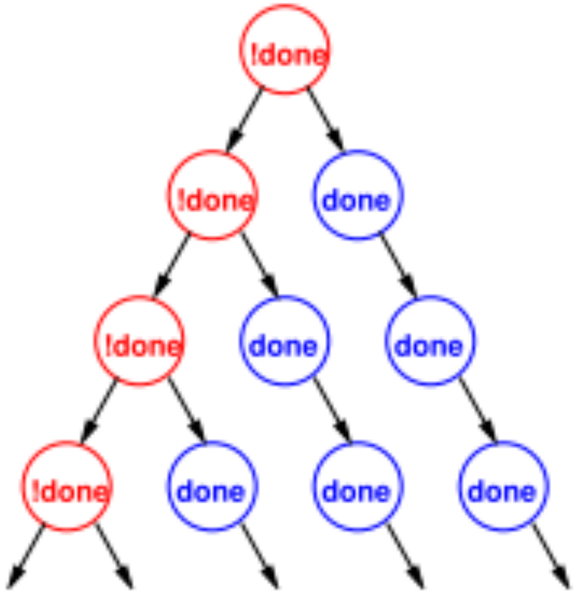


We assume tree can have infinite height

Call it a Computation Tree

Computation Tree for Statecharts





Shows all possible executions

Each actual execution will follow a single path consisting of a sequence of discrete time steps

Computation Tree Logic

- Language for checking computation trees
- Extends propositional logic with
  temporal operators
- Quantifiers for time-sensitive expressions
- Propositional logic connectives

  $\wedge$ $\neg$ $\vee$ $\rightarrow$

Unary Temporal Operators

On all paths (A)

Next: X*p*

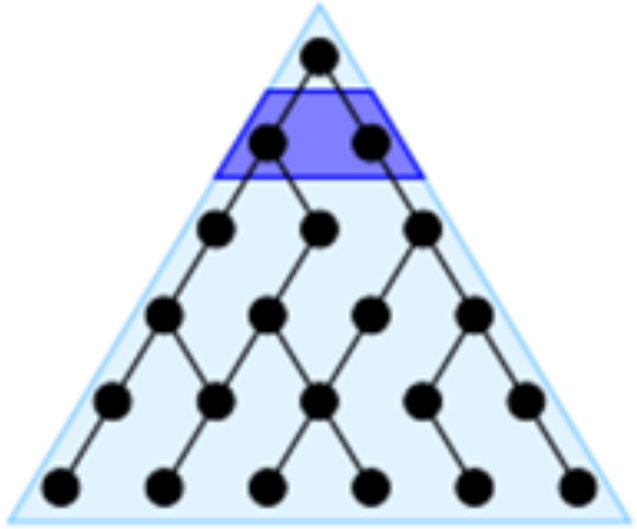
p is true in the next time step

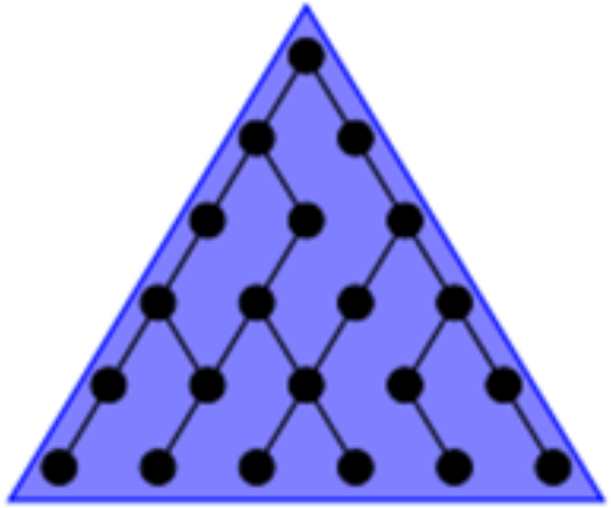
Globally: G*p*

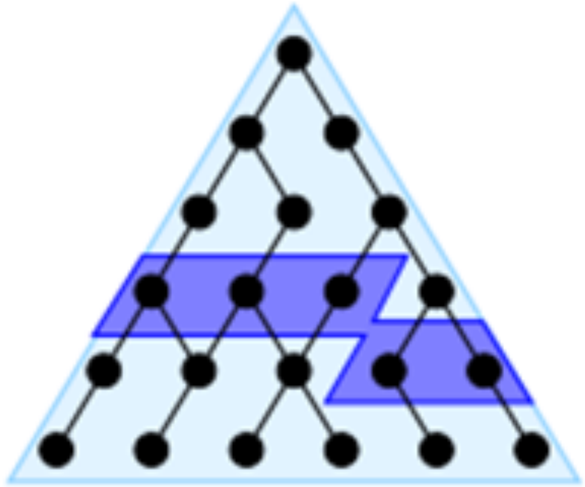
p is true and then forever

Finally: F*p*

p will eventually become true

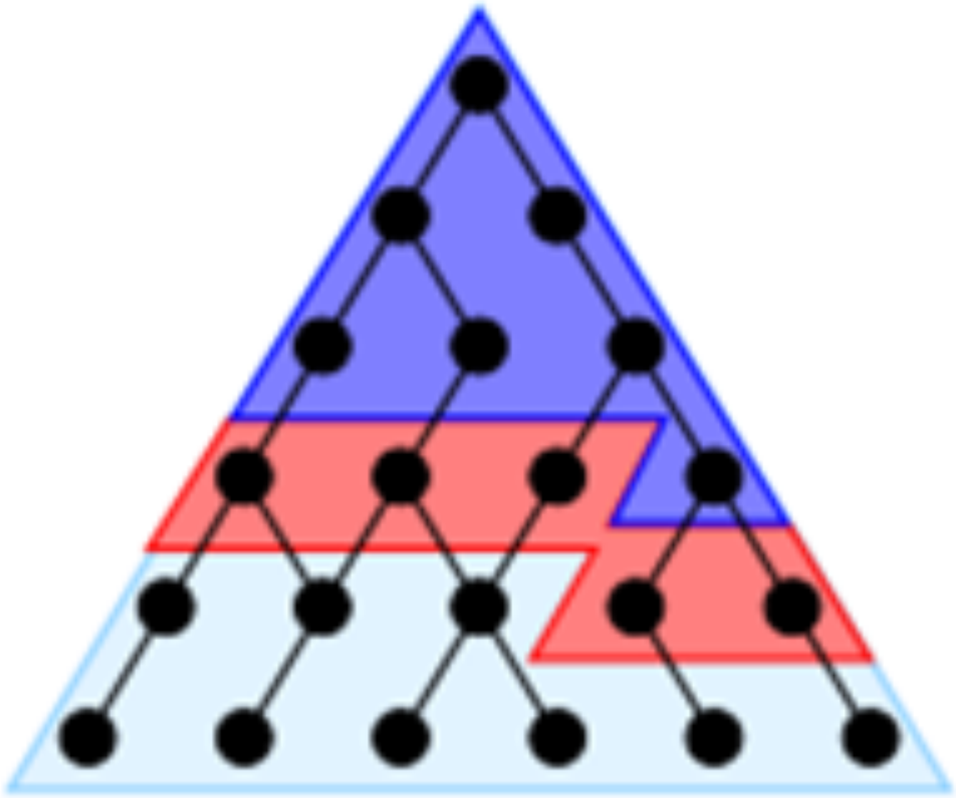






Until

- On all paths



Until: p U q

p is globally true until <u>at least</u> q is true

also q must eventually become true

Path Quantification

- Temporal operators just say what is true on a single execution(sequence)
- We want to talk about ***execution possibilities***

Forall paths**: A***p*

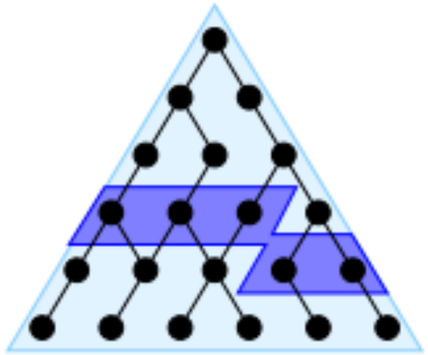
p is true for every possible execution path

There exists a path**: E***p*

p is true for at least one execution path

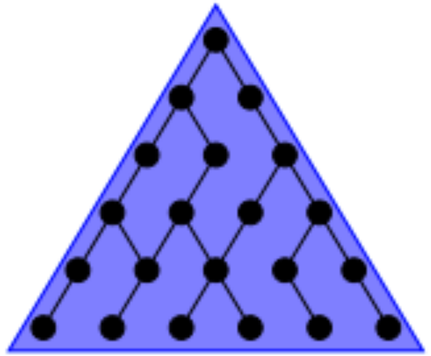
Computation Tree Logic

finally p



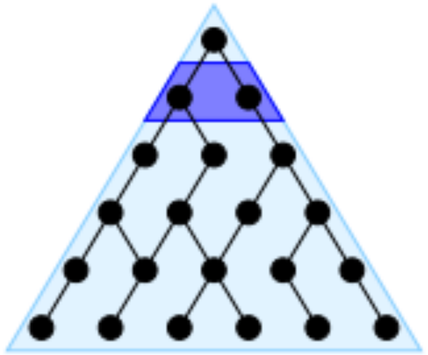
AF p

globally p



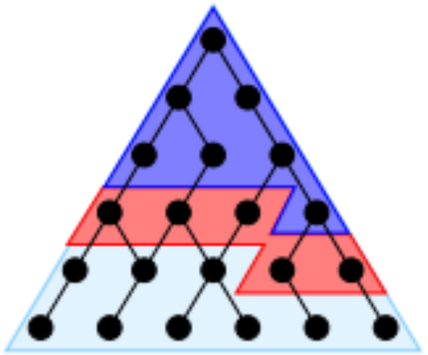
AG p

next p

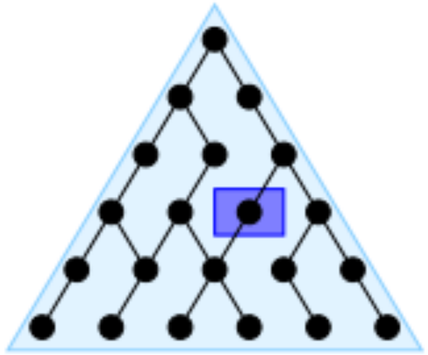


AX p

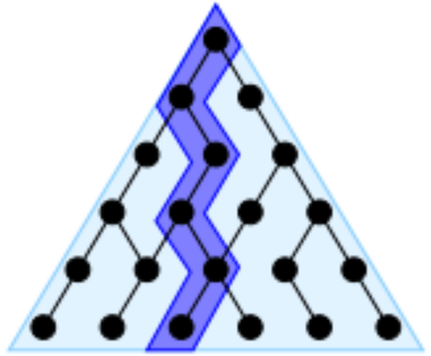
p until q



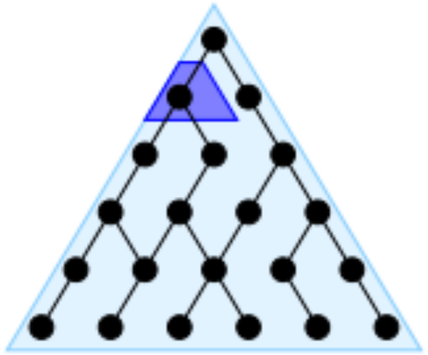
A[p U q]



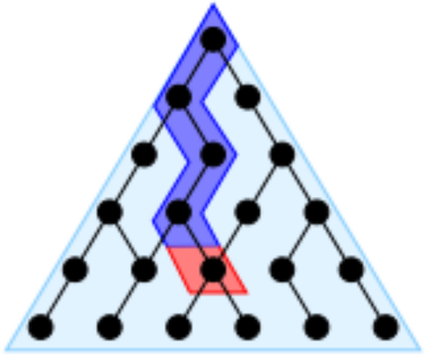
EF p



EG p



EX p



E[p U q]

Examples from Wikipedia

- Let "P" mean "I like chocolate" and Q mean "It's warm outside."
- **AG**.P
  - "I will like chocolate from now on, no matter what happens."
- **EF**.P
  - "It's possible I may like chocolate some day, at least for one day."
- **AF.EG**.P
  - “It's always possible (AF) that I will suddenly start liking chocolate for the rest of time." (Note: not just the rest of my life, since my life is finite, while **G** is infinite).

Examples from Wikipedia

- **EG.AF**.P
  - "This is a critical time in my life. Depending on what happens (E), it's possible that for the rest of time (G), there will always be some time in the future (AF) when I will like chocolate. However, if the wrong thing happens next, then all bets are off and there's no guarantee about whether I'll ever like chocolate."

- **A**(P**U**Q)
  - "From now until it's warm outside, I will like chocolate every single day. Once it's warm outside, all bets are off as to whether I'll like chocolate anymore. Oh, and it's guaranteed to be warm outside eventually, even if only for a single day."

- **E**((**EX**.P)**U**(**AG**.Q))
  - "It's possible that: there will eventually come a time when it will be warm forever (AG.Q) and that before that time there will always be *some* way to get me to like chocolate the next day (EX.P)."

Interesting Properties

- We would like to *verify* or check some relevant properties
  - Safety: Some proposition cannot be true (bad things cannot happen).
  - Liveness: Some proposition will eventually be true (good things will happen).
  - Fairness: Constrains the execution paths. E.g. every state is reached (Absolute fairness), every enabled state is executed (Strong fairness)

Safety Property Examples

$\mathbf{AG}\ \neg(\text{temp} > 1000)$

$\mathbf{AG}\ \neg(\text{NS\_GREEN} \wedge \mathbf{AX}\ \text{EW\_GREEN})$

Liveness Property Examples

$\mathbf{AF}$ win_lottery

$\mathbf{AG}$ (requestQuit → AF quit)

Fairness Property Example

AG (**AF** skytrain_arrives)

How is this different from:

AF skytrain_arrives

?