Software Verification

Lecture 9: Model Checking

Carlo A. Furia
Program Verification: the very idea

P: a program

max (a, b: INTEGER): INTEGER is
do
  if a > b then
    Result := a
  else
    Result := b
end
end

S: a specification

require
ture
ensure
Result >= a
Result >= b

Does P ⊨ S hold?

The Program Verification problem:

- Given: a program P and a specification S
- Determine: if every execution of P, for every value of input parameters, satisfies S
Why is Verification Difficult?

The very nature of universal (Turing-complete) computation entails the impossibility of deciding automatically the program verification problem.

\[ \text{Does } \text{TM}(P) \models F(S) \text{ hold? } \]

UNDECIDABLE
Decidability vs. Expressiveness Trade-Off

If we restrict the expressiveness of:

- the computational model
  and/or
- the specification language

the verification problem can become decidable

Does \( P \models S \) hold?

Def. Expressiveness: capability of describing extensive classes of:

- computations
- properties
Verification of Finite-state Programs
Verification of Finite-state Programs

In Model Checking we typically assume:

- finite-state programs
  - every variable has finite domain
- monadic first-order logic
  - restricted first-order logic fragment where the ordering of state values during a computation can be expressed

\[ P \vdash S \] is Decidable

\( P \): a finite-state program \hspace{1cm} \( S \): a monadic first-order specification

\textbf{Does} \( P \vdash S \) \textbf{hold?}
Verification of Finite-state Programs

In Model Checking we typically assume:

- finite-state programs
  - equivalently: finite-state automata of some kind
- monadic first-order logic
  - equivalently: temporal logic of some kind

P: a program  
\( \Downarrow \)  
FSA(P): a finite-state automaton  
\( \Downarrow \)  
TL(S): a temporal-logic formula

Does \( FSA(P) \models TL(S) \) hold?  
DECIDABLE
is_locked: BOOLEAN

toggle_lock: is
do
    is_locked := not is_locked
end

ensure
is_locked = not old is_locked

⊧ □ (toggle_lock ⇔ X toggle_lock)

P: a program
FSA(P): a finite-state automaton

S: a specification
TL(S): a temporal-logic formula
Finite-state Programs in the Real World

Can finite-state models capture significant aspects of real programs? Yes!

A few examples:

- Behavior of hardware
  - inherently finite-state

- Concurrency aspects
  - access to critical regions, scheduling of processes, ...

- Security aspects
  - access policies, protocols, ...

- Reactive systems
  - ongoing interaction between software and physical environment
How to guarantee that the finite-state abstraction of an infinite-state program is accurate?

- In hardware verification, the real system is finite-state, so no abstraction is needed
- The finite-state model can be built and verified before the real implementation is produced
  - A formal high-level model
  - Increased confidence in some key features of the system under development
  - Model-driven development: the implementation is derived (almost) automatically from the high-level finite-state model
Is the Abstraction Correct?

How to guarantee that the finite-state abstraction of an infinite-state program is accurate?

- **Software model-checking**: the abstraction is built automatically and refined iteratively until we can guarantee that it is an accurate model of the real implementation for the properties under verification.
The Model-checking Paradigm
The Model-Checking Paradigm

The Model Checking problem:

- **Given**: a finite-state automaton $A$ and a temporal-logic formula $F$
- **Determine**: if every run of $A$ satisfies $F$ or not
  - if not, provide a counterexample:
    a run of $A$ where $F$ does not hold

$A$: a finite-state automaton

$F$: a temporal-logic formula

$\models \Box (\text{toggle}\_\text{lock} \leftrightarrow \mathbf{X} \text{toggle}\_\text{lock})$
The Model-Checking Paradigm

A: a finite-state automaton  
F: a temporal-logic formula

\[ F \models \Box (\text{toggle\_lock} \leftrightarrow X \text{toggle\_lock}) \]

Different choices are possible for the kinds of automata and of formulae.

- We now describe more details for linear-time model-checking where:
  - A is a (nondeterministic) finite state automaton
  - F is a propositional linear temporal logic formula
Finite State Automata: Syntax
Def. Nondeterministic Finite State Automaton (FSA):

A tuple \([\Sigma, S, I, \rho, F]\):

- \(\Sigma\): finite nonempty (input) alphabet
- \(S\): finite nonempty set of states
- \(I \subseteq S\): set of initial states
- \(F \subseteq S\): set of accepting states
- \(\rho: S \times \Sigma \rightarrow 2^S\): transition function
Finite State Automata: Syntax

Def. Nondeterministic Finite State Automaton (FSA):
a tuple \([\Sigma, S, I, \rho, F]\):
- \(\Sigma\): finite nonempty (input) alphabet
- \(S\): finite nonempty set of states
- \(I \subseteq S\): set of initial states
- \(F \subseteq S\): set of accepting states
- \(\rho: S \times \Sigma \to 2^S\): transition function

- \(\Sigma = \{ \text{pull, push, turn\_on, turn\_off, start, stop, cook} \}\)
- \(S = \{ \text{closed-off, open-off, closed-on, open-on, closed-cooking} \}\)
- \(I = \{ \text{closed-off} \}\)
- \(F = \{ \text{closed-off} \}\)
- \(\rho(\text{closed-off, turn\_on}) = \{ \text{closed-on} \}\)
- \(\rho(\ldots, \ldots) = \ldots\)

- Deterministic, in this example ("microwave oven")
Finite State Automata: Semantics

Accepting run
\[ r = \text{closed-off closed-on closed-cooking} \]
\[ \text{closed-cooking closed-on closed-off} \]
over input word
\[ w = \text{turn_on start cook stop turn_off} \]

Rejecting run
\[ r' = \text{closed-off open-off closed-off} \]
\[ \text{closed-on} \]
over input word
\[ w' = \text{pull push turn_on} \]
Def. An accepting run of an FSA $A = [\Sigma, S, I, \rho, F]$ over input word $w = w(1) w(2) \ldots w(n) \in \Sigma^*$ is a sequence $r = r(0) r(1) r(2) \ldots r(n) \in S^*$ of states such that:

- it starts from an initial state: $r(0) \in I$
- it ends in an accepting state: $r(n) \in F$
- it respects the transition function:
  $$r(i+1) \in \rho(r(i), w(i)) \text{ for all } 0 \leq i < n$$
Finite State Automata: Semantics

Def. An accepting run of an FSA $A= [\Sigma, S, I, \rho, F]$ over input word $w = w(1) w(2) ... w(n) \in \Sigma^*$ is a sequence $r = r(0) r(1) r(2) ... r(n) \in S^*$ of states such that:

- it starts from an initial state: $r(0) \in I$
- it ends in an accepting state: $r(n) \in F$
- it respects the transition function: $r(i+1) \in \rho(r(i), w(i))$ for all $0 \leq i < n$

- **Accepting run**
  
  $r = $ closed-off closed-on closed-cooking closed-cooking closed-on closed-off

- **Over input word**
  
  $w = $ turn_on start cook stop turn_off

- **In practice**: any path on the directed graph that starts in an initial state and ends in an accepting state
Def. Any FSA $A = [\Sigma, S, I, \rho, F]$ defines a set of input words $\langle A \rangle$:

$$\langle A \rangle \triangleq \{ w \in \Sigma^* \mid \text{there is an accepting run of } A \text{ over } w \}$$

$\langle A \rangle$ is called the language of $A$
Def. Any FSA $A = [\Sigma, S, I, \rho, F]$ defines a set of input words $\langle A \rangle$:

$\langle A \rangle \triangleq \{ w \in \Sigma^* \mid \text{there is an accepting run of } A \text{ over } w \}$

$\langle A \rangle$ is called the language of $A$

With regular expressions:

$\langle A \rangle = ( (\text{pull push})^* (\text{turn}_\text{on} (\text{pull push})^* (\text{start cook}^* \text{ stop})^* (\text{pull push})^* \text{ turn}_\text{off})^* )^*$
Def. Propositional Linear Temporal Logic (LTL) formulae are defined by the grammar:

\[ F ::= p \mid \neg F \mid F \land G \mid X F \mid F \cup G \]

with \( p \in P \) any atomic proposition from a fixed set \( P \).

Temporal (modal) operators:
- next: \( X F \)
- until: \( F \cup G \)
- release: \( F R G \triangleq \neg (\neg F \cup \neg G) \)
- eventually: \( \diamond F \triangleq \text{True} \cup F \)
- always: \( \Box F \triangleq \neg \diamond \neg F \)

Propositional connectives:
- not: \( \neg F \)
- and: \( F \land G \)
- or: \( F \lor G \triangleq \neg (\neg F \land \neg G) \)
- implies: \( F \Rightarrow G \triangleq \neg F \lor G \)
- iff: \( F \Leftrightarrow G \triangleq (F \Rightarrow G) \land (G \Rightarrow F) \)
Def. Propositional Linear Temporal Logic (LTL) formulae are defined by the grammar:

\[ F ::= p \mid \neg F \mid F \land G \mid XF \mid F U G \]

with \( p \in P \) any atomic proposition from a fixed set \( P \).

\[ \Box (\text{start} \Rightarrow X (\text{cook} U \text{stop})) \]
Linear Temporal Logic: Semantics

- □ (start)
- □ (X cook)
- □ (X cook)
- cook ∧ □ (X cook)
- stop ∧ start
Linear Temporal Logic: Semantics

- □ ( start )
  - start, start, start, ...

- □ ( X cook )

- X ( cook )

- cook ∧ □ ( X cook )

- stop ∧ start

- □ ( X cook )
Linear Temporal Logic: Semantics

- □ ( start )
  start, start, start, ...
- X ( cook )
  [any], cook, [any], ...
- □ ( X cook )
- cook ∧ □ ( X cook )
- stop ∧ start
Linear Temporal Logic: Semantics

- $\square (\text{start} )$
  start, start, start, ...

- $\mathcal{X} (\text{cook} )$
  [any], cook, [any], ...

- $\square (\mathcal{X} \text{cook} )$
  [any], cook, cook, cook, ...

- $\text{cook} \land \square (\mathcal{X} \text{cook} )$
  cook, cook, cook, ...

- stop $\land$ start
Linear Temporal Logic: Semantics

- □ (start)
  start, start, start, ...

- X (cook)
  [any], cook, [any], ...

- □ (X cook)
  [any], cook, cook, cook, ...

- cook ∧ □ (X cook)
  cook, cook, cook, ...

- stop ∧ start
  Ø
Linear Temporal Logic: Semantics

Def. A word \( w = w(1) \ldots w(n) \in P^* \) satisfies an LTL formula \( F \) at position \( 1 \leq i \leq n \), denoted \( w, i \models F \), under the following conditions:

- \( w, i \models p \) iff \( p = w(i) \)
- \( w, i \models \neg F \) iff \( w, i \not\models F \) does not hold
- \( w, i \models F \land G \) iff both \( w, i \models F \) and \( w, i \models G \) hold
- \( w, i \models X F \) iff \( i < n \) and \( w, i+1 \models F \)
  
  • i.e., \( F \) holds in the next step
- \( w, i \models F U G \) iff for some \( i \leq j \leq n \) it is: \( w, j \models G \) and for all \( i \leq k < j \) it is \( w, k \models F \)
  
  • i.e., \( F \) holds until \( G \) will hold
Linear Temporal Logic: Semantics

For derived operators:

- \( w, i \models \diamondsuit F \) iff for some \( i \leq j \leq n \) it is: \( w, j \not\models F \)
  
  i.e., \( F \) holds eventually (in the future)

- \( w, i \models \square F \) iff for all \( i \leq j \leq n \) it is: \( w, j \not\models F \)
  
  i.e., \( F \) holds always (in the future)
Def. Satisfaction:

\[ w \models F \equiv w, 1 \models F \]

i.e., word w satisfies formula F initially

Def. Any LTL formula F defines a set of words \( \langle F \rangle \):

\[ \langle F \rangle \equiv \{ w \in P^* \mid w \models F \} \]

\( \langle F \rangle \) is called the language of F
Def. Any LTL formula $F$ defines a set of words $\langle F \rangle$:

$$\langle F \rangle \triangleq \{ w \in P^* \mid w \Downarrow F \}$$

$\langle F \rangle$ is called the language of $F$

$$\langle \Box \text{start} \rangle = \text{start, start, start, start, ...}$$
Verification as Emptiness Checking

The Model Checking problem:

- **Given**: a finite-state automaton $A$ and a temporal-logic formula $F$
- **Determine**: if every run of $A$ satisfies $F$ or not
  - if not, also provide a counterexample:
    a run of $A$ where $F$ does not hold

$\langle A \rangle = \text{words accepted by } A$  \quad  \langle F \rangle = \text{words satisfying } F$
Verification as Emptiness Checking

\[ A: \text{a finite-state automaton} \quad F: \text{a temporal-logic formula} \]

\[ A \models F \quad \iff \quad \langle A \rangle = \text{words accepted by } A \quad \langle F \rangle = \text{words satisfying } F \]

\[ A \models F \quad \text{means: \quad \text{“every accepting run of } A \text{ produces}} \]
\[ \text{a word that satisfies } F \text{“} \]

\[ A \models F \quad \iff \quad w \in \langle A \rangle \text{ implies } w \in \langle F \rangle \]

\[ \iff \quad \langle A \rangle \subseteq \langle F \rangle \]

\[ \iff \quad \langle A \rangle \cap \langle F \rangle^c = \emptyset \]

\[ \iff \quad \langle A \rangle \cap \langle \neg F \rangle = \emptyset \]
Automata-theoretic Model Checking

An semantic view of the Model Checking problem:

- **Given:** a finite-state automaton $A$ and a temporal-logic formula $F$
- if $\langle A \rangle \cap \langle \neg F \rangle$ is empty then every run of $A$ satisfies $F$
- if $\langle A \rangle \cap \langle \neg F \rangle$ is not empty then some run of $A$ does not satisfy $F$
  - any member of the nonempty intersection $\langle A \rangle \cap \langle \neg F \rangle$ is a counterexample
Automata-theoretic Model Checking

How to check $\langle A \rangle \cap \langle \neg F \rangle = \emptyset$ algorithmically (given $A$, $F$)?

Combination of three different algorithms:

- **LTL2FSA**: given LTL formula $F$ build automaton $a(F)$ such that $\langle F \rangle = \langle a(F) \rangle$

- **FSA-Intersection**: given automata $A$, $B$ build automaton $C$ such that $\langle A \rangle \cap \langle B \rangle = \langle C \rangle$

- **FSA-Emptiness**: given automaton $A$ check whether $\langle A \rangle = \emptyset$ is the case
Given an LTL formula $F$, it is always possible to build automatically an FSA $a(F)$ that accepts precisely the same words that satisfy $F$.

There are various algorithms to achieve this, with various degrees of sophistication and efficiency. Let us skip the details and just demonstrate the idea on an example.
LTL2FSA: from LTL to FSA

□ ( start ⇒ X (cook U stop) )

- Always:
  - when start occurs:
    - stop will occur in the future and
    - cook holds until the occurrence of stop
LTL2FSA: from LTL to FSA

□ ( start ⇒ X (cook U stop) )

- Always:
  - when start occurs:
    - stop will occur in the future and
    - cook holds until the occurrence of stop

As long as start does not occur, everything's fine.
LTL2FSA: from LTL to FSA

□ (start ⇒ X (cook U stop))

- Always:
  - when start occurs:
    - stop will occur in the future and
    - cook holds until the occurrence of stop

As long as start does not occur, everything’s fine.

start occurs: move to a different (non-accepting) state and start monitoring.
LTL2FSA: from LTL to FSA

\[ \square ( \text{start} \Rightarrow X (\text{cook} U \text{stop}) ) \]

- Always:
  - when start occurs:
    - stop will occur in the future and
    - cook holds until the occurrence of stop

As long as start does not occur, everything's fine.

start occurs: move to a different (non-accepting) state and start monitoring.

stop must occurs in the future for things to be fine.
LTL2FSA: from LTL to FSA

\( (\text{start} \Rightarrow X (\text{cook} U \text{stop})) \)

- Always:
  - when start occurs:
    - stop will occur in the future and
    - cook holds until the occurrence of stop

As long as start does not occur, everything's fine.

start occurs: move to a different (non-accepting) state and start monitoring.

stop must occur in the future for things to be fine.

cook can occur before stop does.
LTL2FSA: from LTL to FSA

□ (∀ start ⇒ ∃! (cook U stop))

- Always:
  - when start occurs:
    - stop will occur in the future and
    - cook holds until the occurrence of stop

Corner cases:

- which events satisfy ¬start?
- what happens if neither cook nor stop occur in B2?
LTL2FSA: complete the transitions

\[ \square ( \text{start} \Rightarrow X (\text{cook} \cup \text{stop}) ) \]

- **Always:**
  - **when start occurs:**
    - stop will occur in the future and
    - cook holds until the occurrence of stop
  - if this doesn't happen, fail
LTL2FSA: complement

□ ( start ⇒ X (cook U stop) )

¬□ ( start ⇒ X (cook U stop) )
≡
◊ ( start ∧ X (¬cook R ¬stop))

- Always:
  - when start occurs:
    - stop will occur in the future and
    - cook holds until the occurrence of stop
  - if this doesn't happen, fail

- Sometimes:
  - start occurs and from that moment on:
    - cook becomes false after stop
Given automata \( A, B \) it is always possible to build automatically an FSA \( C \) that accepts precisely the words that both \( A \) and \( B \) accept.

Automaton \( C \) represents all possible parallel runs of \( A \) and \( B \) where a word is accepted if and only if both \( A \) and \( B \) accept it. The (simple) construction is called “product automaton”.
FSA-Intersection: running FSA in parallel
FSA-Intersection: running FSA in parallel
FSA-Intersection: running FSA in parallel
FSA-Intersection: running FSA in parallel

[Diagram showing the intersection of two finite state automata (FSAs) followed by an equal sign, indicating the result of the intersection.]
FSA-Intersection: running FSA in parallel

Diagram showing the intersection of two FSA states: closed_off, open_off, closed_on, and open_on. The intersection process is illustrated with transitions between these states, indicating the parallel execution of the FSA processes.
FSA-Intersection: running FSA in parallel
Def. Given FSA $A = [\Sigma, S^A, I^A, \rho^A, F^A]$ and $B = [\Sigma, S^B, I^B, \rho^B, F^B]$

let $C \triangleq A \times B \triangleq [\Sigma^C, S^C, I^C, \rho^C, F^C]$ be defined as:

- $\Sigma^C \triangleq \Sigma$
- $S^C \triangleq S^A \times S^B$
- $I^C \triangleq \{(s, t) \mid s \in I^A \text{ and } t \in I^B\}$
- $\rho^C((s, t), \sigma) \triangleq \{(s', t') \mid s' \in \rho^A(s, \sigma) \text{ and } t' \in \rho^B(t, \sigma)\}$
- $F^C \triangleq \{(s, t) \mid s \in F^A \text{ and } t \in F^B\}$

Theorem. $\langle A \times B \rangle = \langle A \rangle \cap \langle B \rangle$
Given an automaton $A$ it is always possible to check automatically if it accepts some word.

It suffices to check whether any final state can be reached starting from any initial state.

This amount to checking reachability on the graph representing the automaton: if a path is found, it corresponds to an accepted word; otherwise the automaton accepts an empty language.
FSA-Emptiness: node reachability

It suffices to check whether any final state can be reached starting from any initial state.

From the initial state $B_1$ both accepting states can be reached.

Correspondingly we find the accepted words:
- start
- start cook cook
- start stop start
- ...

The accepted language is not empty.
Automata-theoretic Model Checking Algorithm:

- **Given**: a finite-state automaton $A$ and a temporal-logic formula $F$

1. **TL2FSA**: build “tableau” automaton $a(\neg F)$
2. **FSA-Intersection**: build “product” automaton $A \times a(\neg F)$
3. **FSA-Emptiness**: check whether $A \times a(\neg F) = \emptyset$

- **If** $A \times a(\neg F) = \emptyset$ **then** any run of $A$ satisfies $F$
- **If** $A \times a(\neg F) \neq \emptyset$ **then** show a run of $A$ where $F$ does not hold
Automata-theoretic Model Checking

doesn't accept anything, hence we have verified:

\[ \square (\text{start} \Rightarrow X (\text{cook} \cup \text{stop})) \]
Transition Systems vs. Finite State Automata
Transition Systems

- A slight variant of the model-checking framework uses finite-state transition systems instead of finite-state automata to model the finite-state program/system.
  - Kripke structures is another name for finite-state transition systems.
- A finite-state transition system is a finite-state automaton where propositions are associated to states rather than transition.
- The finite-state transition system and finite-state automaton models are essentially equivalent and it is easy to switch from one to the other.
- The finite-state transition system model is closer to the notion of finite-state program, but the automaton model is more amenable to variants and generalizations (see e.g., class on real-time model-checking).
Automaton vs. Transition System
Automaton vs. Transition System

□ ( start ⇒ X (cook U stop) )

□ (closed-cooking ⇒
X (closed-cooking U closed-on))
Transition System vs. Automaton

Diagram of a transition system and an automaton with states A, B, and C. The diagram on the left shows the transition system, and the diagram on the right shows the automaton.
n_to_n (n: INTEGER): INTEGER
require 0 ≤ n ≤ 2
local i: INTEGER

do

from i := n ; Result := 1

until i = 0

loop

Result := Result * n

i := i - 1

end

ensure Result = n^n end
forever (b: BOOLEAN)
  local old, new: BOOLEAN
  do
    from old := b ; new := not b
    until old = new
  loop
    old := new
    new := not old
  end
end
Variants of the Model-Checking Algorithm
Variants of the Model-Checking Algorithm

The basic model-checking algorithm:

- TL2FSA: build automaton $a(\neg F)$
- FSA-Intersection: build automaton $A \times a(\neg F)$
- FSA-Emptiness: check whether $A \times a(\neg F) = \emptyset$

Can be refined into different variants:

- Explicit-state model-checking
- Symbolic (BDD-based) model-checking
- Bounded (SAT-based) model-checking

The variants differ in how they represent automata and formulae and how they analyze them. Hybrid approaches are also possible.
Explicit-state Model Checking

Explicit-state model-checking represents automata explicitly as graphs:

- **TL2FSA**: build automaton $a(\neg F)$
  - the automaton is represented as a graph
- **FSA-Intersection**: build automaton $A \times a(\neg F)$
  - the intersection is usually built *on-the-fly* while checking emptiness, because the product automaton can be large
- **FSA-Emptiness**: check whether $A \times a(\neg F) = \emptyset$
  - a search on the expanded intersection graph looks for reachable accepting nodes

**SPIN** is an example of explicit-state model checker.
Symbolic model-checking represents automata implicitly (symbolically) through their transition functions encoded as BDDs (Binary Decision Diagrams):

- A BDD is an efficient representation of Boolean functions (i.e., truth tables) as acyclic graphs.
- Logic operations (e.g., conjunction, negation) can be performed efficiently directly on BDDs.
Symbolic Model Checking

Logic operations (e.g., conjunction, negation) can be performed efficiently directly on BDDs

- **TL2FSA**: build automaton $a(\neg F)$
  - the transition function of the automaton is represented as a BDD
- **FSA-Intersection**: build automaton $A \times a(\neg F)$
  - the intersection is a BDD built by manipulating the two BDDs
- **FSA-Emptiness**: check whether $A \times a(\neg F) = \emptyset$
  - emptiness checking is also performed directly on the BDD
    - it amount to reduction to a canonical form and then comparison with the canonical BDD for unsatisfiable Boolean functions

**SMV** is an example of symbolic model checker.
Bounded model-checking considers all paths of bounded size on the automaton and represents them as a propositional formula. Propositional formulas are then checked for satisfiability with SAT-solvers (i.e., automatic provers for propositional satisfiability).

- The bound \( k \) of the path size is an additional input to the model-checking problem with respect to standard model-checking. However, if the bound is “large enough” the problem is equivalent to standard model-checking.

- Even if the encoding as a propositional formula is quite large, SAT-solvers can handle huge (e.g., \( > 10^5 \) propositions) formulas efficiently.

NP-completeness should never scare the compiler writer.

-- Andrew W. Appel
Bounded Model Checking

- **TL2FSA**: build automaton $a(\neg F)$
  - the LTL formula is translated directly into a propositional formula $p(\neg F)$

- **FSA-Intersection**: build automaton $A \times a(\neg F)$
  - the product of two propositional formulas is simply their conjunction $p(A) \land p(\neg F)$

- **FSA-Emptiness**: check whether $A \times a(\neg F) = \emptyset$
  - emptiness checking is equivalent to satisfiability checking of $p(A) \land p(\neg F)$

nuSMV and Zot are examples of bounded model checkers.
Variants of the Model-Checking Approach
The Model Checking problem:

- **Given**: a finite-state automaton \( A \) and a temporal-logic formula \( F \)
- **Determine**: if any run of \( A \) satisfies \( F \) or not
  - if not, also provide a counterexample: a run of \( A \) where \( F \) does not hold

The **general** problem can be refined into variants, according to the **nature** of \( A \) and \( F \).

- The **same** generic automata-theoretic **solution**
  (\( \text{TL2FSA} \rightarrow \text{Intersection} \rightarrow \text{Emptiness} \))

applies to **any** of these variants
(modulo some technicalities)
Variants of the Model-Checking Problem

The general problem can be refined into variants, according to the nature of $A$ and $F$.

**Classes of automata:**
- Finite State Automata (FSA)
- Büchi Automata (BA)
- Alternating Automata (AA)
- ...

**Classes of temporal logic:**
- Linear-time temporal logic
- Branching-time temporal logic
- Temporal logic with past operators
- ...

Classes are non-disjoint

Classes are non-disjoint
Automata Classes

- **Finite-state Automata (FSA)**
  - those presented in this lecture
  - FSA runs correspond to **finite words** (words of finite length)

- **Büchi Automata (BA)**
  - named after Julius Büchi (Swiss logician, ETH graduate)
  - BA runs correspond to **infinite words** (words of unbounded length)
    - this complicates the definitions of acceptance, product, and complement, as well as the algorithm for emptiness
  - infinite words are needed to model:
    - **reactive systems**: ongoing interaction with environment
      - e.g., control system, interactive protocol, etc.
    - **liveness** and fairness
      - e.g., “process P will not starve”
  - the most common presentation of linear-time model-checking uses BA
Temporal Logic Classes

- **Linear-time** Temporal Logic (LTL)
  - the one presented in this lecture
  - LTL formulae express properties of *linear sequences*, that is words
    - linear: every element has only one possible successor
    - linear time: every step has only one possible “future”

- **Branching-time** Temporal Logic
  - includes *path quantifiers* in the syntax
  - for example **CTL** (Computation Tree Logic):
    - $F ::= p \mid \neg F \mid F \land G \mid \exists X F \mid \forall X F \mid F \mathbin{\mu} G \mid F \mathbin{\nu} G$
  - branching-time formulae express properties of *branching structures*, that is trees
    - branching: an element can have multiple possible successors
    - branching time: a step can have many possible “futures”
  - e.g.: $\exists \diamond p$: “there exists a path where $p$ eventually holds”
Linear vs. Branching

LTL and CTL have different strengths and weaknesses

- **Expressiveness**: LTL and CTL have incomparable expressive power
  - CTL formula $\forall \Diamond \forall \Box p$:
    “p will stabilize at True within a bounded amount of time”
    doesn't have an equivalent LTL formula
  - LTL formula $\Diamond \Box p$:
    “p is ultimately True in every computation”
    doesn't have an equivalent CTL formula
  - see infinite computation tree
    (p holds precisely in **green** nodes)