Lecture 2

Specifying Requirements

Natalia Sidorova

Overview of the lecture

- The need for temporal logics
- Temporal operators
- Practical use
- Typical requirements

Mutual exclusion protocol

Typical properties of a mutual exclusion protocol

- It is never the case that two (or more) processes occupy their critical section at the same time
- Whenever a process wants to enter its critical section, it eventually will do so (absence of individual starvation)

How to specify these properties in an unambiguous and precise way?

Traffic light

Typical properties of a traffic light:

- Once green, the light cannot become immediately red
- Eventually the light will be red again
- Once green, the light becomes red after being yellow for some time between being green and being red

How to specify these properties in an unambiguous and precise way?

Elevator

Typical properties of an elevator:

- Any elevator request must ultimately be satisfied
- The elevator never misses a floor for which a request is pending without satisfying this request

How to specify these properties in an unambiguous and precise way?

Note that all these properties concern the dynamic behaviour of the system!

The need for temporal logics

Years 1950-s – 70-s: Sequential programs.
Pre- and post-conditions are enough to specify requirements.

Nowadays: Reactive, distributed, concurrent systems:

- Business processes
- Telecommunication systems
- Web-based systems
- . . .

Not only begin- and end-states are of importance, but also what happens during the computation

Temporal and modal logics

- Modal logics were originally developed by philosophers to study different modes of truth (“necessarily ϕ” or “possibly ϕ”).
- Temporal logic (TL) is a special kind of modal logic where truth values of assertions vary over time.
- Typical modalities (temporal operators) are
  - “sometimes ϕ” is true if property ϕ holds at some future moment
  - “always ϕ” is true if property ϕ holds at all future moments
- TL is often used to specify and verify reactive systems, i.e. systems that continuously interact with the environment (Pnueli, 1977)

Two views on reactive systems

- The system generates a set of traces.
  - the models of temporal logics are infinite sequences of states or transitions
  - LTL (linear time temporal logic) [Manna, Pnueli]
- The system generates a tree, where the branching points represent nondeterminism.
  - the models of temporal logics are infinite trees
  - CTL (computation tree logic) [Clarke, Emerson]

Temporal logics

- Basic building blocks: atomic propositions
  - on states (used in this lecture), or
  - on actions (out of consideration in this lecture)
- TL; (P)LTL (linear time)
- CTL (branching time) - is not considered here
- CTL^* (includes both LTL and CTL)

Atomic propositions

are declarative sentences that can be true or false

- “The sun is shining today.”
- “There is a party tonight.”
- “x+y = z”

Atomic propositions are boolean expressions that can use

- data variables (integers, sets, etc.),
- control variables (locations),
- constants (0,1,2,. . . ,$\emptyset$,. . .) and
- predicate symbols ($\leq, \geq, \in, \subseteq$).

State formulas (assertions)

are formulas that are evaluated over a single state of a system

For state s and formula p
$s \models p$ iff $s[p] = \mathrm{T}$

We say

- p holds at s
- s satisfies p
- s is a p-state

State formulas (example)

For state $s : \{x : 4, y : 1\}$

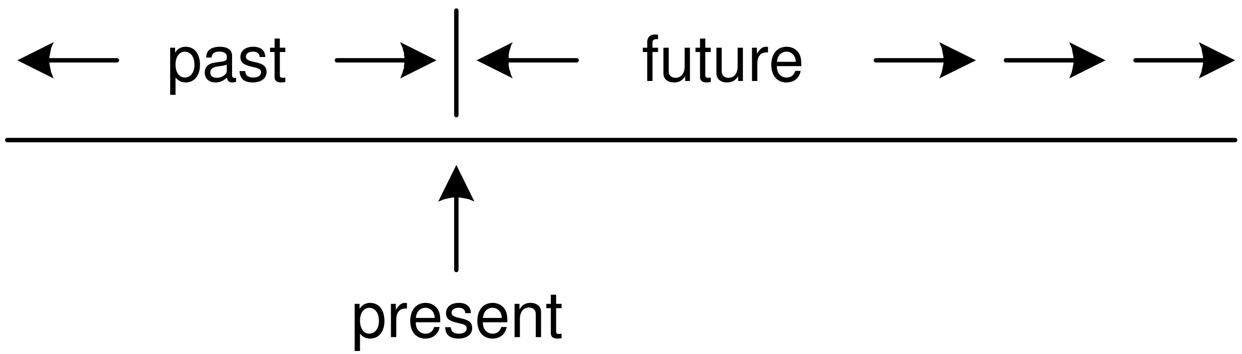
- $s \models x = 0 \vee y = 1$
- $s \not\models x = 0 \wedge y = 1$

Temporal logic (TL)

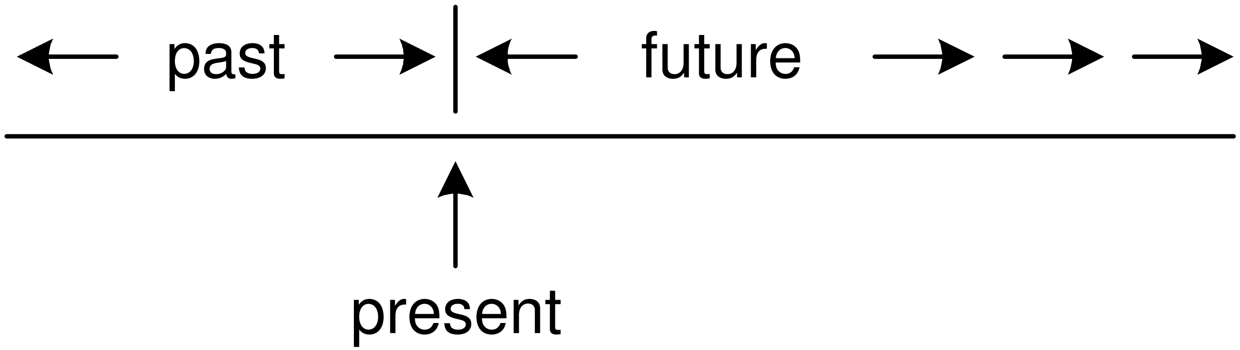
is a formalism for specifying sequences of states.

TL = state formulas + temporal operators

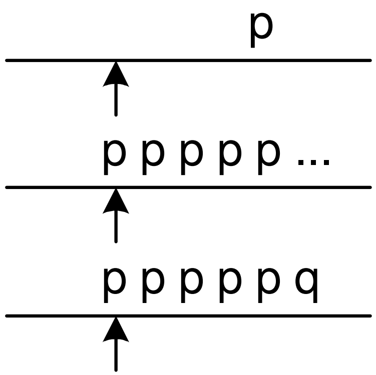
- Future temporal operators to express e.g. that something good will eventually happen in the future, or nothing bad will happen in the future.
- Past temporal operators: to express the properties about the past of the system.



Future temporal operators

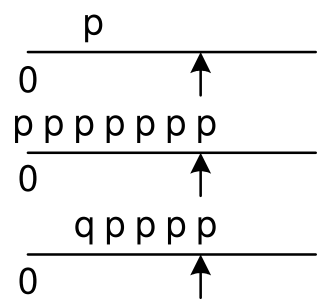


- $\Diamond p$ — Eventually p
- $\Box p$ — Henceforth p (always p)
- $p\,\mathcal{U} q$ — p until q



- $p\mathcal{W}q$ — p waiting-for (unless) q — $\Box p \vee p\,\mathcal{U} q$
- $\bigcirc p$ — Next p, i.e. p holds in the *next* state

Past temporal operators



- $\diamondminus\, p$ — Once p
- $\boxminus\, p$ — So-far p
- $p\,\mathcal{S}q$ — p since q
- $p\mathcal{B}q$ — p back-to q — $\boxminus\, p \vee p\,\mathcal{S}q$
- $\ominus p$ — Previously p (at the previous state, p holds) (false at position 0)
- $\bigcirc\!\!\!\!\sim\, p$ — Before p (true at position 0)

Examples

$$\Box(x > 0 \longrightarrow \Diamond\!\!\!\!\!-\;\, y = x)$$

$$p\,\mathcal{U}q \longrightarrow \Diamond q$$

Temporal logic: semantics

Temporal formulas are evaluated over a model which is an infinite sequence of states

$\sigma : s_0, s_1, s_2, \ldots$

The semantics of TL-formula p at a position $j \geq 0$ in a model σ,

$(\sigma, j) \models p$ — formula p holds at position j of model σ —

is defined by induction on p.

Temporal logic: semantics (2)

- For a state formula p, $(\sigma, j) \models p \quad \Leftrightarrow \quad s_j \models p$
- $(\sigma, j) \models p \vee q \quad \Leftrightarrow \quad s_j \models p$ or $s_j \models q$,
- etc.

- $(\sigma, j) \models \Box p \quad \Leftrightarrow \quad$ for all $k \geq j, \quad (\sigma, k) \models p$
- $(\sigma, j) \models \Diamond p \quad \Leftrightarrow \quad$ for some $k \geq j, \quad (\sigma, k) \models p$
- $(\sigma, j) \models p\,\mathcal{U} q \quad \Leftrightarrow \quad$ for some $k \geq j, \quad (\sigma, k) \models q$,
  and for all $i, \; j \leq i < k, \quad (\sigma, i) \models p$
- $(\sigma, j) \models p \mathcal{W} q \quad \Leftrightarrow \quad (\sigma, j) \models p\,\mathcal{U} q$ or $(\sigma, j) \models \Box p$
- $(\sigma, j) \models \bigcirc p \quad \Leftrightarrow \quad (\sigma, j+1) \models p$

Temporal logic: semantics (3)

- $(\sigma, j) \models \boxminus p \quad \Leftrightarrow \quad$ for all $0 \leq k \leq j, \quad (\sigma, k) \models p$
- $(\sigma, j) \models \diamondminus p \quad \Leftrightarrow \quad$ for some $0 \leq k \leq j, \quad (\sigma, k) \models p$
- $(\sigma, j) \models p \mathcal{S} q \quad \Leftrightarrow \quad$ for some $k, \quad 0 \leq k \leq j, \quad (\sigma, k) \models q$,
  and for all $i, \quad j < i \leq k, \quad (\sigma, i) \models p$
- $(\sigma, j) \models p \mathcal{B} q \quad \Leftrightarrow \quad (\sigma, j) \models p \mathcal{S} q$ or $(\sigma, j) \models \boxminus p$
- $(\sigma, j) \models \ominus p \quad \Leftrightarrow \quad (\sigma, j-1) \models p$
- $(\sigma, j) \models \circledtilde\, p \quad \Leftrightarrow \quad$ either $j = 0$ or else $(\sigma, j-1) \models p$

Simple examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $p \rightarrow \Diamond q$

Simple examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $p \longrightarrow \Diamond q$
  if initially p then eventually q

Simple examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \vDash \phi$.

- $p \to \Diamond q$
  if initially p then eventually q
- $\Box(p \to \Diamond q)$

Simple examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \vDash \phi$.

- $p \longrightarrow \Diamond q$
  if initially p then eventually q
- $\Box(p \longrightarrow \Diamond q)$
  every p is eventually followed by a q

Simple examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $p \longrightarrow \Diamond q$
  if initially p then eventually q
- $\Box(p \longrightarrow \Diamond q)$
  every p is eventually followed by a q
- $\Box\Diamond q$

Simple examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \vDash \phi$.

- $p \longrightarrow \Diamond q$
  if initially p then eventually q
- $\Box(p \longrightarrow \Diamond q)$
  every p is eventually followed by a q
- $\Box\Diamond q$
  every state is eventually followed by a q, i.e., infinitely many q's

Some more examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $\Diamond\Box q$

Some more examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \vDash \phi$.

- $\Diamond\Box q$
  eventually permanently q, i.e., finitely many $\neg q$

Some more examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $\Diamond\Box q$
  eventually permanently q, i.e., finitely many $\neg q$
- $\Box\Diamond p \rightarrow \Box\Diamond q$

Some more examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $\Diamond\Box q$
  eventually permanently q, i.e., finitely many $\neg q$
- $\Box\Diamond p \longrightarrow \Box\Diamond q$
  if there are infinitely many p's then there are infinitely many q's

Some more examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $\Diamond\Box q$
  eventually permanently q, i.e., finitely many $\neg q$
- $\Box\Diamond p \rightarrow \Box\Diamond q$
  if there are infinitely many p's then there are infinitely many q's
- $(\neg p)\mathcal{W}q$

Some more examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $\Diamond\Box q$
  eventually permanently q, i.e., finitely many $\neg q$
- $\Box\Diamond p \longrightarrow \Box\Diamond q$
  if there are infinitely many p's then there are infinitely many q's
- $(\neg p)\mathcal{W}q$
  q precedes p (if p occurs)

And the last two examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $\Box(p \rightarrow \bigcirc p)$

And the last two examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $\Box(p \rightarrow \bigcirc p)$
  once p, always p

And the last two examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $\Box(p \rightarrow \bigcirc p)$
  once p, always p
- $\Box(q \rightarrow \diamondminus p)$

And the last two examples

Given temporal formula ϕ, describe model σ such that $(\sigma, 0) \models \phi$.

- $\Box(p \rightarrow \bigcirc p)$
  once p, always p
- $\Box(q \rightarrow \diamondminus p)$
  every q is preceded by a p

Classification of properties

[L. Lamport 1973]

Safety properties

- All finite prefixes of a trace satisfy a certain requirement
- “No bad things will happen”
- Violation can be detected in finite time

Liveness (progress) properties

- “Something good will happen eventually”
- depends on fairness conditions in non-trivial cases

Most commonly used patterns

Statistics over 555 requirement specifications
[M. Dwyer et al., 1998]

response:	$\Box(p \rightarrow \Diamond q)$	43.4%
universality:	$\Box p$	19.8%
global absence:	$\Box \neg p$	7.4%
precedence:	$\Box \neg p \vee \neg p \mathcal{U} q$	4.5%
absence between:	$\Box((p \wedge \neg q \wedge \Diamond q) \rightarrow (\neg r \,\mathcal{U} q))$	3.2%
absence after:	$\Box(q \rightarrow \Box \neg p)$	2.1%
existence:	$\Diamond p$	2.1%

Fairness hypothesis

- Alternating bit protocol: channels may loose messages.
- Requirements:
  - every message received was earlier sent
  - the order of messages is preserved
  - any emitted message is eventually received

Fairness hypothesis

- Alternating bit protocol: channels may loose messages.
- Requirements:
  - every message received was earlier sent
  - the order of messages is preserved
  - any emitted message is eventually received
    — does not hold in general, since channels may systematically loose all the messages

Fairness hypothesis

- Alternating bit protocol: channels may loose messages.
- Requirements:
  - every message received was earlier sent
  - the order of messages is preserved
  - any emitted message is eventually received — does not hold in general, since channels may systematically loose all the messages
- Fairness hypothesis: from time to time channels do deliver messages

Fairness hypothesis

- Alternating bit protocol: channels may loose messages.
- Requirements:
  - every message received was earlier sent
  - the order of messages is preserved
  - any emitted message is eventually received — does not hold in general, since channels may systematically loose all the messages
- Fairness hypothesis: from time to time channels do deliver messages
  $\Box\Diamond\neg\text{loss} \rightarrow \Box(\text{emmited} \rightarrow \Diamond\text{received})$

Fairness and nondeterminism

- Nondeterminism: a free choice between several actions leading to different states.
- Such a choice is often assumed to be fair: not inclined to omit one option.
- A die with six faces is repeatedly thrown.
  In fact we have equiprobability then (ideally).
  Modelling that would require stochastic propositions and models.
- Fairness is a simple abstraction of probabilistic properties.

Strong and weak fairness

- Fairness properties:
  "If S is continually requested, then S will be (infinitely often) granted.
- Weak fairness:
  continually requested = without interruption
  $\Diamond\Box requested \rightarrow \Box\Diamond granted$
- Strong fairness:
  continually requested = infinitely often
  $\Box\Diamond requested \rightarrow \Box\Diamond granted$
- Strong fairness implies weak fairness

Variations in requirement style

- Allowable behaviour: define what a correctly functioning system is able to do
- Violations: define what a correctly functioning system can never do

Checking PLTL-properties in Spin

PLTL: propositional linear time temporal logic
requirements on sequences of states should hold for all traces

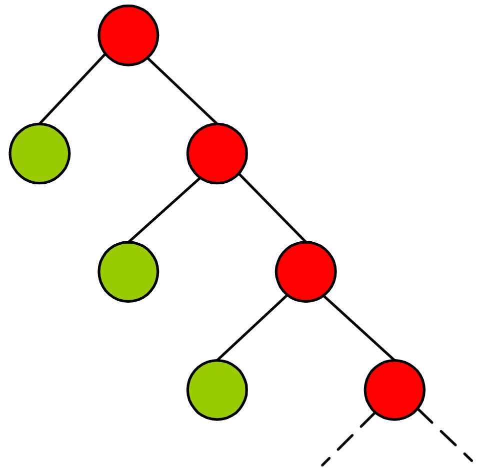
Only future time temporal operations

No next state operator

Does linear time always suffice?

Often but not always

- At any instant of any execution it is possible to reach a state where p holds.

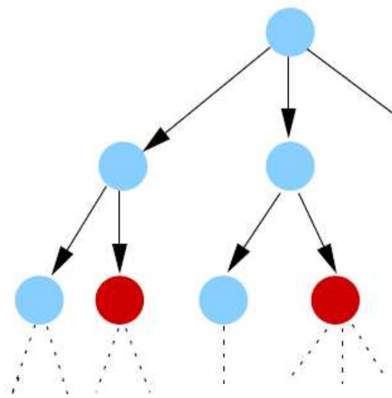


CTL*

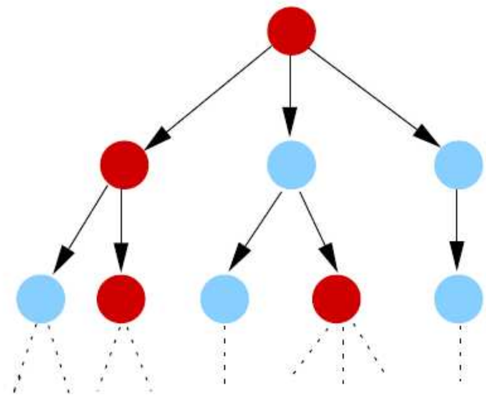
Extended Computation Tree Logic

- Temporal combinators:
  - Xp — the next state satisfies p ($\bigcirc p$)
  - Fp — a future state satisfies p ($\Diamond p$)
  - Gp — all future states satisfy p ($\Box p$)
  - U and W with the same meaning as before
- Path quantifiers:
  - Aϕ — all the execution out of the current state satisfy ϕ
  - Eϕ — there exists an execution out of the current state that satisfy ϕ

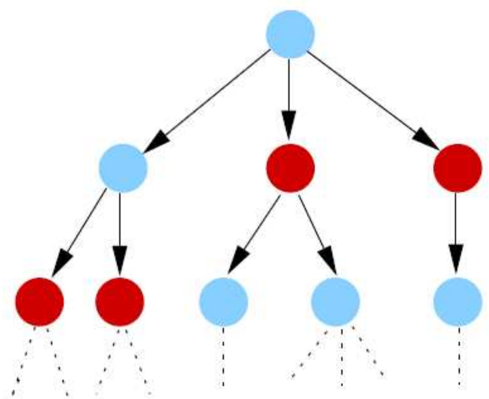
Examples



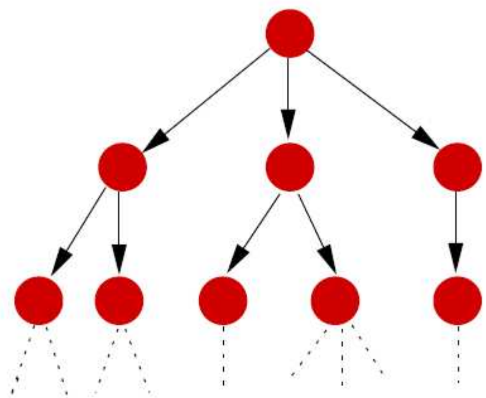
EF *red*



EG *red*



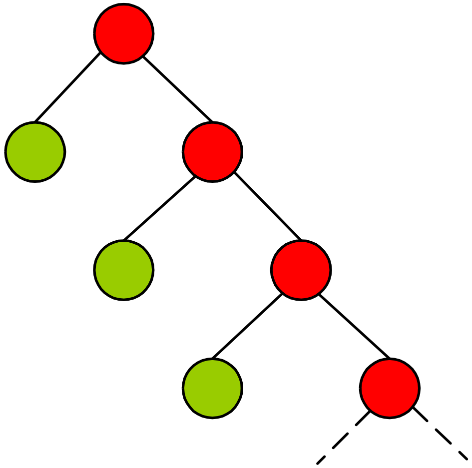
AF *red*



AG *red*

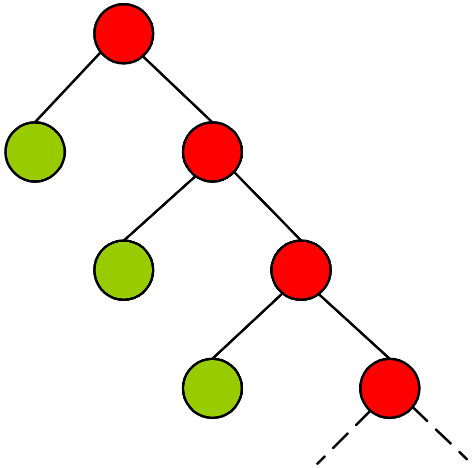
Which formula expresses this?

- At any instant of any execution it is possible to reach a state where p holds.



Which formula expresses this?

- At any instant of any execution it is possible to reach a state where p holds.



AG EF p

Strong and weak fairness in CTL*

- Fairness properties:
  "If S is continually requested, then S will be (infinitely often) granted.
- Weak fairness:
  continually requested = without interruption

Strong and weak fairness in CTL*

- Fairness properties:
  "If S is continually requested, then S will be (infinitely often) granted.
- Weak fairness:
  continually requested = without interruption
  FG $enabled \rightarrow$ GF $executed$

Strong and weak fairness in CTL*

- Fairness properties:
  "If S is continually requested, then S will be (infinitely often) granted.
- Weak fairness:
  continually requested = without interruption
  FG $enabled \rightarrow$ GF $executed$
- Strong fairness:
  continually requested = infinitely often

Strong and weak fairness in CTL*

- Fairness properties:
  "If S is continually requested, then S will be (infinitely often) granted.
- Weak fairness:
  continually requested = without interruption
  FG $enabled \rightarrow$ GF $executed$
- Strong fairness:
  continually requested = infinitely often
  GF $enabled \rightarrow$ GF $executed$

To know more:

Chapter 2 of

Berard et al. "Systems and Software Verification"

Homework

Assignment 1:

- Formulate (meaningful) requirements for some systems. You may use TL, LTL, CTL*.
- Use Spin to check some properties of your models.

Next lecture

- Part 1: modelling: where to start?
- Part 2: Spin tutorial