Langages de spécification – cours 3

Introduction en logique temporelle

Catalin Dima

Specifying temporal properties

- Automata are nice, graphical representations of properties.
- Algorithmics for them turn into graph algorithmics.
  - Essentially reachability and search for strongly connected components.
  - And various constructions of new graphs from smaller ones.
- It's visual, easy to implement, easy to read, but not very easy to write...
  - It's not easy to guess that an automaton represents a responsiveness property.

Regular expressions as a specification language

- Equivalent with finite-state automata.
- Clearly more compact than automata specifications.
- But do we really understand what regular expression mean ?
- Write a regular expression for
  - A property of the type p holds forever on.
  - A property of the type p holds until q holds.
  - A property of the type there exists a point where p holds.
- Wouldn't it be possible to have some primitives that correspond to these ?

Linear Temporal Logic defined

- Extension of propositional logic.
  - Hence all propositional connectives are present.
- Temporal primitives :
  - Next : $X\phi$ or $\bigcirc p$.
  - Until : $\phi \mathcal{U} \psi$.
  - Globally : $G\phi$ or $\square \phi$.
  - Forward : $F\phi$ or $\diamond \phi$.

Linear Temporal Logic defined

- Extension of propositional logic.
  - Hence all propositional connectives are present.
- Temporal primitives :
  - Next : $X\phi$ or $\bigcirc p$.
  - Until : $\phi \mathcal{U} \psi$.
  - Globally : $G\phi$ or $\Box \phi$.
  - Forward : $F\phi$ or $\Diamond \phi$.
- Past time operators can also be employed :
  - Yesterday ϕ held : $Y\phi$ or $\bullet\phi$.
  - ϕ held ever since ψ held : $\phi \mathcal{S} \psi$.
  - Historically or always in the past ϕ held : $H\phi$ or $\blacksquare\phi$.
  - Once ϕ held : $O\phi$ or $\blacklozenge\phi$.

Semantics

- Models of LTL are *runs* $\rho : \mathbb{N} \longrightarrow 2^{AP}$.
  - Equivalently, infinite words over the alphabet 2^{AP}.
- Each atomic proposition has a truth value at each time point :
  - $p \in \rho(0)$ means p holds at the first time instant of the run.
  - $p \in \rho(251)$ means p holds at the 251th time instant of the run.
- Each formula will also be interpreted at each time point along the run :

$$
\begin{array}{ll}
(\rho, i) \models p & \text{if } p \in \rho(i) \\
(\rho, i) \models \phi_1 \wedge \phi_2 & \text{if } (\rho, i) \models \phi_1 \text{ and } (\rho, i) \models \phi_2 \\
(\rho, i) \models \neg\phi & \text{if } (\rho, i) \not\models \phi \\
(\rho, i) \models \bigcirc \phi & \text{if } (\rho, i+1) \models \phi \\
(\rho, i) \models \phi_1 \mathcal{U} \phi_2 & \text{if there exists } j \geq i \text{ with } (\rho, j) \models \phi_2 \\
 & \qquad \text{and for all } i \leq k < j, (\rho, k) \models \phi_1
\end{array}
$$

- Similar semantics for the past operators.
- Examples...

Semantics (2)

- Semantics, continued :

$$(\rho, i) \models \Diamond\, \phi \text{ if there exists } j \in \mathbb{N} \text{ with } (\rho, j) \models \phi$$
$$(\rho, i) \models \Box\, \phi \text{ if for any } j \in \mathbb{N}, (\rho, j) \models \phi$$

- But the first modalities are sufficient :

$$\Diamond\, \phi = \text{true}\, \mathcal{U}\, \phi$$
$$\Box\, \phi = \neg \Diamond \neg \phi$$

Semantics (3)

- Other future-time operators : new formulas read as follows :
  - $\phi_1 \, \mathcal{W} \, \phi_2$: ϕ_1 holds *weakly until* ϕ_2 holds.
  - $\phi_1 \, \mathcal{R} \, \phi_2$: ϕ_2 *releases* ϕ_1.
- Semantics :

$$\phi_1 \, \mathcal{W} \, \phi_2 = \phi_1 \, \mathcal{U} \, \phi_2 \vee \Box \, \phi_1$$

$$\phi_1 \, \mathcal{R} \, \phi_2 = \neg(\neg\phi_1 \, \mathcal{U} \, \neg\phi_2) = \phi_2 \, \mathcal{W}(\phi_1 \wedge \phi_2)$$

Sample formulas

... and their natural-language statement

- Safety formula : $G\phi$.
  - Mutual exclusion : $G\neg(critical_1 \wedge critical_2)$.
- Guarantee formula : $F\phi$.
  - Reachability : $F(chass \wedge loup \wedge chevre \wedge chou)$.
- Intermittence formula : $GF\phi$.
- Persistence formula : $FG\phi$.
  - Convergence : $FG(Voyager - reaches - Alpha - Centauri)$.
- Request-response formula : $G(\phi \longrightarrow F\psi)$.
  - Fairness : $G(ready_i \longrightarrow Fcritical_i)$.

Sample tautologies

- Tautology : formula that is true regardless of the truth values given to the atomic propositions.
- Examples :

$$\neg \bigcirc p \Leftrightarrow \bigcirc \neg p$$
$$\bigcirc p \Rightarrow \Diamond p$$
$$\Diamond \Diamond p \Rightarrow \Diamond p$$
$$\Box(p \wedge q) \Leftrightarrow \Box p \wedge \Box q$$
$$(\Diamond p \Rightarrow \Diamond q) \Rightarrow \Diamond(p \Rightarrow q)$$

- Formulas which are not tautologies :

$$\Diamond(p \wedge q) \Leftrightarrow \Diamond p \wedge \Diamond q$$
$$p\,\mathcal{U}(q\,\mathcal{U}\,r) \Leftrightarrow (p\,\mathcal{U}\,q)\,\mathcal{U}\,r$$

- To prove they are not tautologies, give a counter-model !

Fixpoints

- Until, weak until, release and the others can be defined "inductively" :

$$\Diamond p \equiv p \vee \bigcirc \Diamond p$$
$$\Box p \equiv \ldots ?$$
$$p\,\mathcal{U}\,q \equiv q \vee \left(p \wedge \bigcirc(p\,\mathcal{U}\,q)\right)$$
$$p\,\mathcal{R}\,q \equiv \ldots ?$$

- May define least fixpoints and greatest fixpoints
- The "equation" for $p\,\mathcal{U}\,q$ is $X = q \vee (p \wedge \bigcirc X)$.
  - Constructing the solution works by replacing X with false and iterating.
- The "equation" for $\neg(p\,\mathcal{W}\,q)$ is $X = \neg p \wedge (\neg q \vee \bigcirc X)$.
  - Constructing the solution works by replacing X with true and iterating.

Fixpoint LTL

- Utilize only $\bigcirc$ and boolean connectives.
- And two fixpoint operators :
  - μX, least fixpoint, computed starting with $X :=$ false.
  - νX, greatest fixpoint, computed starting with $X :=$ true.
- What does this mean :
  - $\mu X \nu Y \left(p \wedge \bigcirc(X \vee q \wedge Y)\right)$?...
- Not easy to read...
- But more expressive than temporal logic.

Axiomatizing time

- Axioms and rules for the propositional part (any deduction system).
- Axioms and rules for $\bigcirc$ and $\mathcal{U}$:
  - Distributivity : $\bigcirc\phi \wedge \bigcirc(\phi \longrightarrow \psi) \longrightarrow \bigcirc\psi$.
  - Linear time : $\neg \bigcirc \phi \Leftrightarrow \bigcirc\neg\phi$.
  - Fixpoint axiom for until : $\phi\mathcal{U}\psi \Leftrightarrow \psi \vee (\phi \wedge \bigcirc(\phi\mathcal{U}\psi))$.
  - Next time rule : from ϕ infer $\Box\phi$.
  - Until inference (or induction) rule : from $\phi' \longrightarrow \neg\psi \wedge \bigcirc\phi'$ infer $\phi' \longrightarrow \neg(\phi\mathcal{U}\psi)$.
- $\Box$ and $\Diamond$ can be expressed in terms of $\mathcal{U}$.
- A reduced axiomatic system can also be given only for the fragment with $\bigcirc$ and $\Box$.
  - Replace the fixpoint axiom for until with the fixpoint axiom for $\Box$: $\Box\phi \Leftrightarrow \phi \wedge \bigcirc \Box \phi$.
  - Replace the until inference rule with $\Box$ inference (induction) rule : from $\phi \Rightarrow \psi$ and $\phi \Rightarrow \bigcirc \phi$ infer $\phi \Rightarrow \Box \psi$.

The model-checking problem

- Given a transition system $T = (Q, V, Q_0, \delta, \pi)$ and a formula ϕ, do all the runs of T satisfy ϕ?

$$\forall \rho \in Runs(T), (\rho, 0) \models \phi?$$

- Examples :

Infinite words and repeating states

- A Büchi automaton is a finite-state automaton,
- ... but it works on never-ending sequences of labels.
- There is no “final” state, as an infinite word does not have an end !
- There are repeated states F :

Acceptance condition

To accept an infinite word, a run must pass infinitely often through F

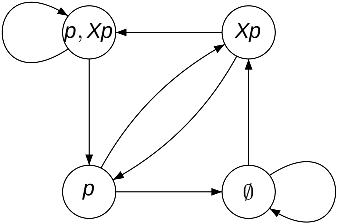
- This is equivalent with requiring that the run must pass infintely often through a state from F ! (ain’t it ?)

Algorithms for Büchi automata

- Emptiness ?
  - Check whether some repeated state is reachable,
  - ... and reaches itself again !
  - Strongly connected component !
- Union ?
  - Easily adaptable from finite automata !
- Intersection ?
  - Try to adapt the intersection algorithm from automata over finite words.
  - ... but which are the repeated states ?...

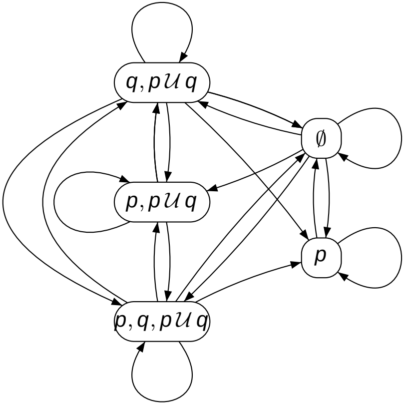
From LTL to Büchi automata

- For each formula ϕ, we may build a Büchi automaton A.
- Construction for $\bigcirc p$ and $\neg \bigcirc p$:



From LTL to Büchi automata (2)

- Construction for $p \mathcal{U} q$ and $\neg(p \mathcal{U} q)$.



- But a Büchi acceptance condition must be added ! Which one ?

Model-checking algorithm

- Construct the automaton A for $\neg\phi$.
  - Spares a complementation step !
- Intersect A with the automaton for the system.
- Check for emptiness.