Systems and Software Verification

Chapter 8. Liveness Properties

Lecturer: JUNBEOM YOO
jbyoo@konkuk.ac.kr
http://dslab.konkuk.ac.kr

Ver. 2.0

8. Liveness Properties

- Liveness property
  - Under certain conditions, some event will ultimately occur.
  - Some happy event will occur in the end.

  - Examples:
    - (L1) " Any request will ultimately be satisfied "
    - (L2) " By keeping on trying, one will eventually succeed "
    - (L3) " If we call on the elevator, it will bound to arrive eventually "
    - (L4) " The light will turn green (some day regardless of the system behavior)"
    - (L5) " After the rain, the sunshine "
    - (L6) " The program will terminate "

  - Two broad family of liveness properties
    1. Simple liveness : <u>*progress*</u> (Chapter 8)
    2. Repeated liveness : <u>*fairness*</u> (Chapter 10)

- Organization of Chapter 8
  - Simple Liveness in Temporal Logic
  - Are Liveness Properties Useful?
  - Liveness in the Model, Liveness in the Properties
  - Verification under Liveness Hypotheses
  - Bounded Liveness

8.1 Simple Liveness in Temporal Logic

- F Φ
  - “ Φ will ultimately occur. ”
  - (L1) “ Any request will ultimately be satisfied ”
    - AG (req ⇒ AF sat)
  - (L7) “ The system can always return to its initial state ”
    - AG EF init
  - P U Q
    - “ Along the execution, we will find a state satisfying Q and P will hold for all the states encountered in the meantime “
    - Regarded as a liveness property
    - $P \ U \ Q \ \equiv \underbrace{F \ Q}_{\text{(liveness)}} \wedge \underbrace{(P \ W \ Q)}_{\text{(safety)}}$
    - A(PUQ) and E(PUQ) are all liveness properties.

8.2 Are Liveness Properties Useful?

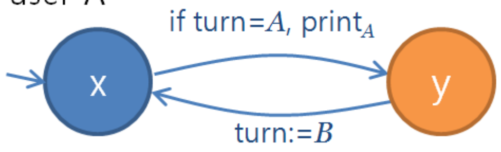
- Abstract liveness properties
  - “ If we call on the elevator, it is bound to arrive eventually “
    - It yields no information, from a utilitarian viewpoint.
    - “Abstract” liveness property
  - “ An event will occur within at most x time unit “
    - It is useful, but became a safety property.
    - “Bounded” liveness property
  - But, it is still useful
    - “Abstract” more general than “concrete”
    - “Abstract” more efficient than “concrete”
    - “Abstract” and “concrete” are not contradictory

8.3 Liveness in the Model, Liveness in the Properties

- Two different roles in the verification process
  1. Liveness *properties* : we wish to verify
  2. Liveness *hypotheses* : we make on the system model

- When we use a mathematical model(automata) to represent a real system,
  - The semantics of the model in face define *implicit safety and liveness hypotheses*.
  - Safety hypothesis :
    - Clear
    - It can flip from q to q' only if it includes a transition going from q to q'.
  - Liveness hypothesis :
    - Not clear
    - The system will chain transitions as long as possible. (to a block state or accepting states)
    - " The system does not terminate without reason, or remain inactive indefinitely without reason. "
    - Can be subtle and cause errors :

The user A



In state x, will always end up wishing printing.
→ Different from the real world's behavior !!!

- <u>One must be aware of the premises of the models used and check their adequacy !</u>

8.4 Verification under Liveness Hypotheses

- Verify that specific model behaviors satisfy a given property :
  - ϕ_v : only the model which the liveness hypotheses hold
  - Ψ : a property

  - Verify $\phi_v \Rightarrow \psi$ is sufficient!!!

  - If ψ is a CTL property
    - AF (E PUQ) → A ($\phi_v \Rightarrow$ FE ($\phi_v \wedge$ P U Q))

8.5 Bounded Liveness

- Bounded liveness property
  - A liveness property that comes with a maximal delay which the desired situation must occur.
  - Safety properties from a theoretical viewpoint.
  - Can be rewritten in a form AG ($\psi_2 \Rightarrow F^{-1}\ \psi_1$)
  - Not as important as safety properties

- Bounded liveness in timed systems
  - Often used in the specification of timed systems (in Chapter 5)
  - Explicit constraints on delays → TCTL !!!
  - (BL1) " The program terminates in less than ten seconds "
    - $AF_{<10s}$ end ← bounded liveness property
    - AG ($\neg$end $\Rightarrow F^{-1}_{<10s}$ start) ← safety property
  - (BL2) " Any request is satisfied in less than five minutes "
    - AG (req $\Rightarrow AF_{<5m}$ sat) ← bounded liveness property
    - AG ($\neg(F^{-1}_{=5m}$req $\wedge$ $G^{-1}_{\leq 5m}\neg$sat) ← safety property