Systems and Software Verification

Chapter 10. Fairness Properties

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

Ver. 2.0

10. Fairness Properties

- Fairness Property
  - Under certain conditions, an event will occur (or will fail to occur) infinitely often
  - Examples:
    - (F1) " The gate will be raised infinitely often"
    - (F2) " If access to a critical section is infinitely often requested, then access will be granted infinitely often "
  - repeated liveness or repeated reachability

- Organization of Chapter 10
  - Fairness in Temporal Logic
  - Fairness and Nondeterminism
  - Fairness Properties and Fairness Hypothesis
  - Strong Fairness and Weak Fairness
  - Fairness in the Model or in the Property?

10.1 Fairness in Temporal Logic

- GF P
  - " We meet a state in which P holds infinitely often "
  - There is no last state in which P holds.
  - Fairness properties cannot be expressed in pure CTL
    - (F1) " The gate will be raised infinitely often"
      → A (GF $\mathrm{gate\_raised}$)
    - (F2) " If access to a critical section is infinitely often requested, then access will be granted infinitely often "
      → A (GF $\mathrm{crit\_req}$ ⇒ FG $\mathrm{crit\_in}$)
  - FCTL or ECTL$^+$
    - CTL + fairness
    - O($|A|$ x $|\phi|^2$)
    - Many tools (like SMV) considers the fairness hypotheses as part of model than choosing FCTL

10.2 Fairness and Nondeterminism

- In practice,
  - Fairness properties are used to describe the form of some nondeterministic sequences
  - " When a nondeterministic choice occurs at some point, it is often assumed to be fair "
  - For example,
    - A die with six faces
    - Its behavior is fair, if it fulfills the property: A (GF 1 ∧ GF 2 ∧ GF 3 ∧ GF 4 ∧ GF 5 ∧ GF 6)
  - Fairness properties can be viewed as an abstraction of probabilistic properties.

10.3 Fairness Properties and Fairness Hypotheses

- Fairness properties are very often used as hypotheses.

- An example:
  - Classical alternating bit protocol
    - A : a transmitter
    - B : a receiver
    - AB : a line for messages
    - BA : a line for message acknowledgements
    - Messages can be lost → non-deterministic behavior of AB and BA

  - Liveness property : " Any emitted message is eventually received "
    - G (emitted ⇒ F received)
    - Fail !!!
    - The model allows to systematically lose all messages.
    - Our original intension : "unreliable" line, not the whole lose → Fairness hypothesis !!!
    - A (GF ¬loss ⇒ G (emitted ⇒ F received))
      fairness hypothesis **liveness property**

  - Repeated liveness property : " If infinitely many messages are emitted, then infinitely many messages will be transmitted "
    repeated liveness property
    - A (GF ¬loss ⇒ (GF emitted ⇒ GF received))
      fairness hypothesis **repeated liveness hypothesis**

10.4 Strong Fairness and Weak Fairness

- Fairness property
  - " If P is continually requested, then P will be granted (infinitely often) "
- Weak fairness
  - Assume that P is requested without interruption
  - (FG $request\_P$) $\Rightarrow$ F P
  - (FG $request\_P$) $\Rightarrow$ GF P
- Strong fairness
  - Assume that P is requested in an infinitely repeated manner, possibly with interruptions
  - (GF $request\_P$) $\Rightarrow$ F P
  - (GF $request\_P$) $\Rightarrow$ GF P
- No difference when using them for model checking of finite systems

10.5 Fairness in the Model or in the Property?

- The best way is
  - Model = automaton + fairness hypotheses
  - Since the second can change independently from the first
  - like SMV model checker