Introduction to Formal Methods

Chapter 9. Deadlock-freeness

Lecturer: JUNBEOM YOO
jbyoo@konkuk.ac.kr

9. Deadlock-freeness

- Deadlock-freeness
  - A special property
  - " The system can never be in a situation on which no progress is possible "

  - Correct property relevant for systems that are supposed to run indefinitely
  - A set of properly identified final states will be required to be deadlock-free.

- Organization of Chapter 9
  - Safety? Liveness?
  - Deadlock-freeness for a Given Automaton
  - Beware of Abstractions!

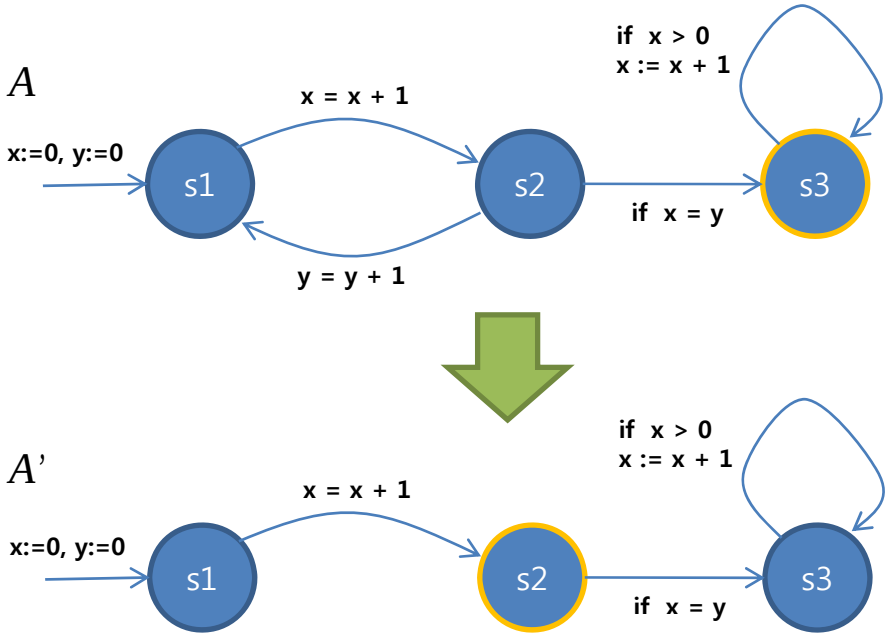
9.1 Safety? Liveness?

- AG EX true
  - " Whatever the state reached may be (AG), there will exist an immediate successor state (EX true) "
  - Not the form of AGϕ^{-1}
  - Deadlock-free is not a safety property.
  - Can be verified if the model checker at our disposal can handle AG EX true.

9.2 Deadlock-freeness for a Given Automaton

- We sometimes think of deadlock-freeness as a safety property
  - For a given automaton, we can describe the deadlock states explicitly.
  - But, it is up to the automaton we obtain.

  - For example,



AG EX true → hold! (liveness property)
AG ¬(s3 ∧ x≤0) → hold! (safety property)

AG EX true → not hold! (liveness property)
AG ¬(s3 ∧ x≤0) → hold! (safety property)

9.3 Beware of Abstractions!