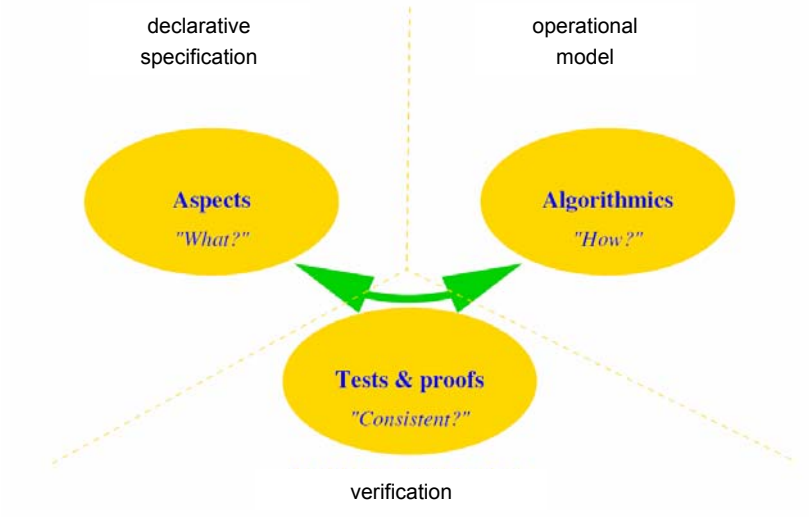
Embedded Systems

Bernd Finkbeiner
Calogero Zarba
Moritz Hahn

Sommersemester 2007

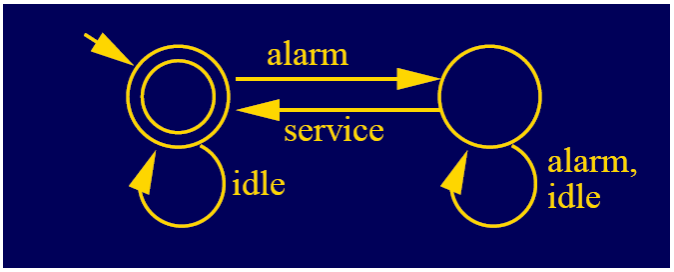
Declarative Specifications & Verification



Linear-time Temporal Logic (LTL)

$\Diamond \varphi$	Eventually	
$\Box \varphi$	Henceforth	
$\varphi \mathcal{U} \psi$	Until	
$\bigcirc \varphi$	Next	

Büchi Automata



Büchi Automata

A **Büchi automaton** over alphabet Σ is a tuple A=(S,I,T,F), where

- S is a finite set of **states**,
- $I \subseteq S$ is a set of **initial states**,
- $T \subseteq S \times \Sigma \times S$ is a set of **transitions**, and
- $F \subseteq S$ is a set of **accepting states**.

A **run** of a Büchi automaton on an infinite sequence $a_1,a_2,a_3,\ldots$ is an infinite sequence of states $s_0,s_1,s_2,\ldots$ such that

- $s_0 \in I$, and
- for all $i \geq 0$, $(s_i, a_{i+1}, s_{i+1}) \in T$

A run is **accepting**, if, for infinitely many i, $s_i \in F$.
An input sequence is **accepted** if it has an accepting run.

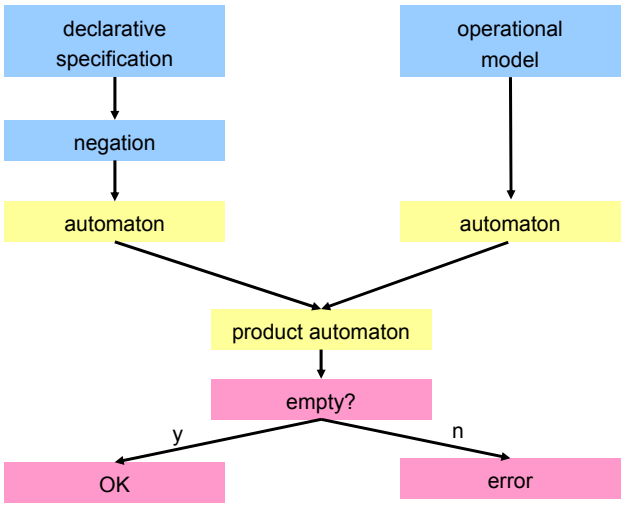
Emptiness of Büchi Automata

Thm: Emptiness of (the language of) a Büchi automaton is decidable.

Algorithm: We need to find out whether states are reachable which are accepting and located in a cycle of the transition relation:

1. Determine the set R of reachable states, e.g. with breadth-first search
2. find the strongly connected components in R, e.g. with Tarjan's algorithm,
3. check these SCCs for containment of an accepting state,
4. report "language is empty" iff no SCC in R contains a state from F.

Model Checking



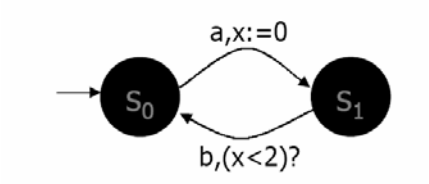
Timed Words

A time sequence $\tau=\tau_1\tau_2\ldots$ is an infinite sequence of time values $\tau_i \in R$ with $\tau_i>0$, satisfying the following constraints:

- Monotonicity: τ increases strictly monotonically so that $\tau_i < \tau_{i+1}$ for all $i \geq 1$.
- Progress: For every $t \in R$, there is some $i \geq 1$ such that $\tau_i > t$.

A timed word over an alphabet Σ is a pair (σ,τ) where $\sigma=\sigma_1\sigma_2\ldots$ is an infinite word over Σ and τ is a time sequence. A timed language over Σ is a set of timed words over Σ.

Timed Transition Tables



$$\{((ab)^{\omega},\tau) \mid \forall i.(\tau_{2i} < \tau_{2i-1} + 2)\}$$

Timed Transition Tables

A **timed transition table** A over alphabet Σ is a tuple (S,I,X,T), where

- S is a finite set of **states**,
- $I \subseteq S$ is a set of **initial states**,
- X is a finite set of **clocks**, and
- $T \subseteq S \times \Sigma \times C(X) \times 2^X \times S$ is a set of **transitions**.
  (s,a,δ,λ,s') represents a transition from state s to state s'
  on input symbol a.

  The **guard** δ is a clock constraint over C.
  The set λ identifies the clocks to be **reset**.

  Clock constraints C(X): $x \leq c \mid c \leq x \mid \neg\delta \mid \delta_1 \wedge \delta_2$,
  where $x \in X$, c a non-negative rational number,
  δ_1, δ_2 are clock constraints.