Prof. Bernd Finkbeiner, Ph.D.
Dr. Swen Jacobs
Maximilian Schwenger

Saarland University
Reactive Systems Group
Due: **28.06.2018** 10:15

Embedded Systems (SS 2018)

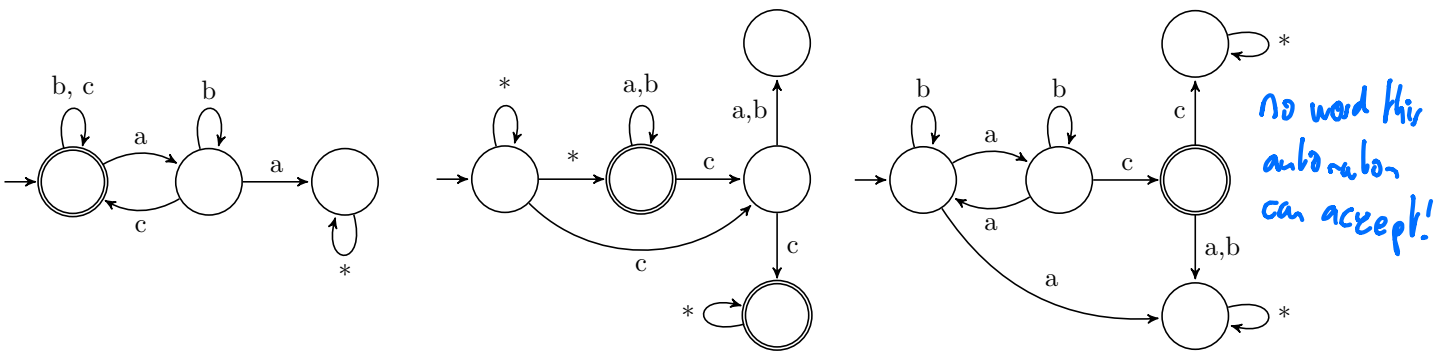
Problem Set F

Note: The material for Problem F3 will be covered in Tuesday's lecture.

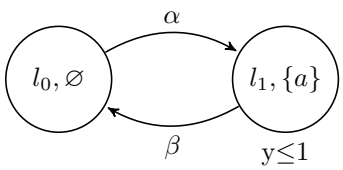
Problem F1: Büchi Automata (5 Points) if not mentioned, then automata non-deterministic

a) Briefly describe the difference between Büchi Automata and deterministic finite automata (DFA).

b) Find an LTL formula describing the words accepted by the following Büchi Automata with $\Sigma = \{a, b, c\}$. An edge with label $*$ can be taken with any input symbol. Hint: Unary operators have precedence over binary operators. For everything else, use parentheses.



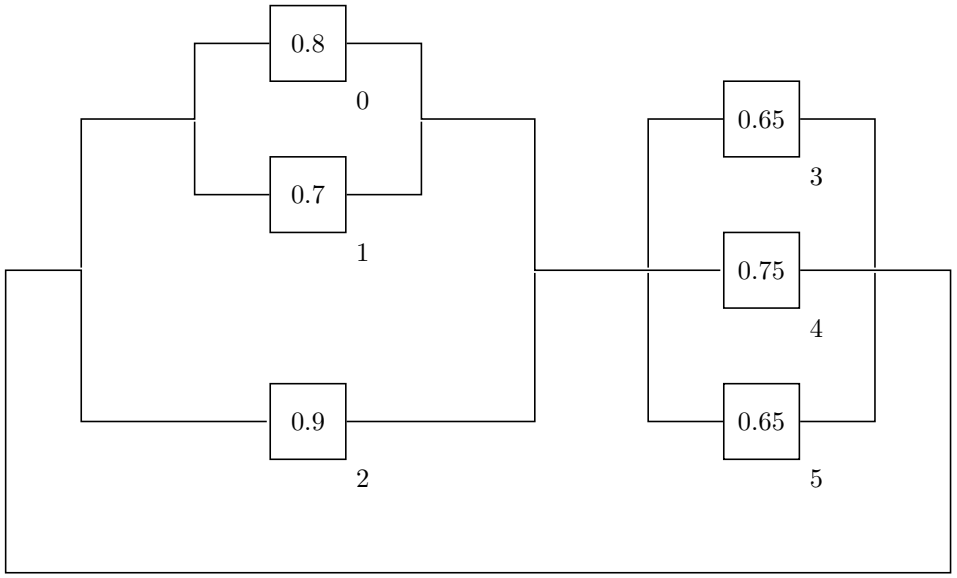
Problem F2: Model Checking (8 Points)
Consider the LTL specification $\varphi := \mathbf{FG}\neg a$ and the following timed automaton $\mathcal{T}$:



Use model checking to verify whether the automaton satisfies φ. For that, perform the following steps:

1. Construct the region graph $[\![\mathcal{T}]\!]_r$ for $\mathcal{T}$.
2. Negate φ.
3. Construct a Büchi automaton $\mathcal{B}_{\neg\varphi}$.
4. Construct $[\![\mathcal{T}]\!]_r \parallel \mathcal{B}_{\neg\varphi}$.
5. Search for reachable loops with accepting states in $[\![\mathcal{T}]\!]_r \parallel \mathcal{B}_{\neg\varphi}$

Problem F3: Reliability Analysis (9 Points)
Consider the following reliability diagram of a system. Each block represents a component. The number in the block states its reliability, the number next to it denotes its id.



a) Compute the overall reliability of the system. For this, first compute the reliability of suitable subsystems. Show your computation steps and use the ids of blocks for easier referencing.

b) A minimal cut set is a size-minimal set of components whose collective failure causes a failure of the whole system. Determine the set $\mathcal{S}$ of all minimal cut sets of the given system.

c) The following formula computes a lower bound on the reliability of the system:

$$R(t) \geq 1 - \sum_{S \in \mathcal{S}} \prod_{i \in S} (1 - R_i(t))$$

Compute the bound and compare it against the exact bound computed before.

d) Compare both algorithms. Which one would you prefer and why?

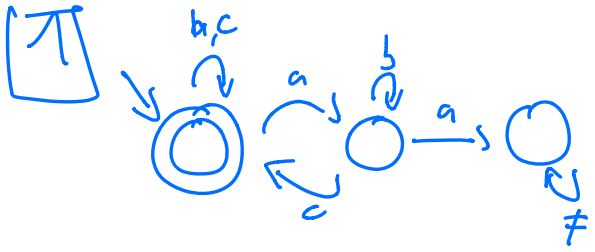
Problem F4: Deductive Verification (5 **Bonus** Points)
Consider the following program:

@pre $\|s\| = len \wedge (\forall i \colon 0 < i < len \implies s[i] \in [0, 255])$
@post $rv \iff \left(\sum_{i=0}^{len} s[i]\right) \cdot len^{-1} \geq 200$

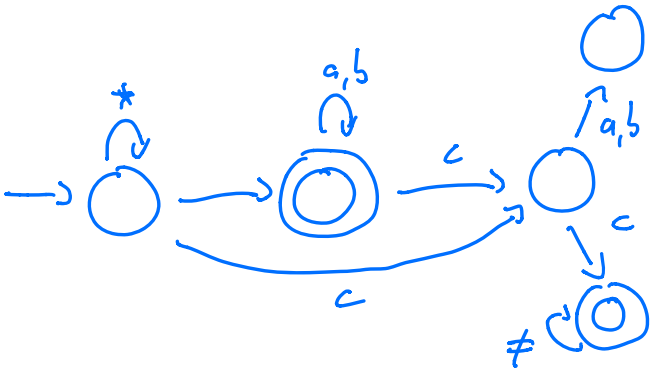
```
bool ftv(int[] s, int len) {
  int accu := 0;
  for (int i = 0; i < len; i := i + 1) {
    accu := accu + s[i];
    if (accu div len >= 200) {
      return true;
    }
  }
  int avg = accu div len;
  bool res = avg >= 200
  return res;
}
```

a) Verify the validity of the post-condition after the execution of the program assuming the pre-condition holds.

Tutorial:



$\delta(a \to X(b \mathcal{U} c))$



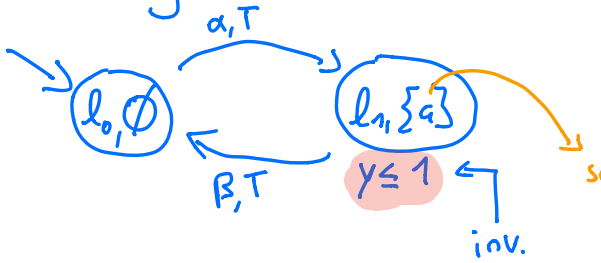
$\delta F(c \wedge Xc) \vee F\delta(a \vee b)$

. . .

1

2 $\varphi = FG\neg a$

e.g.: a b c a b c ... ↓ ... b c b c b c

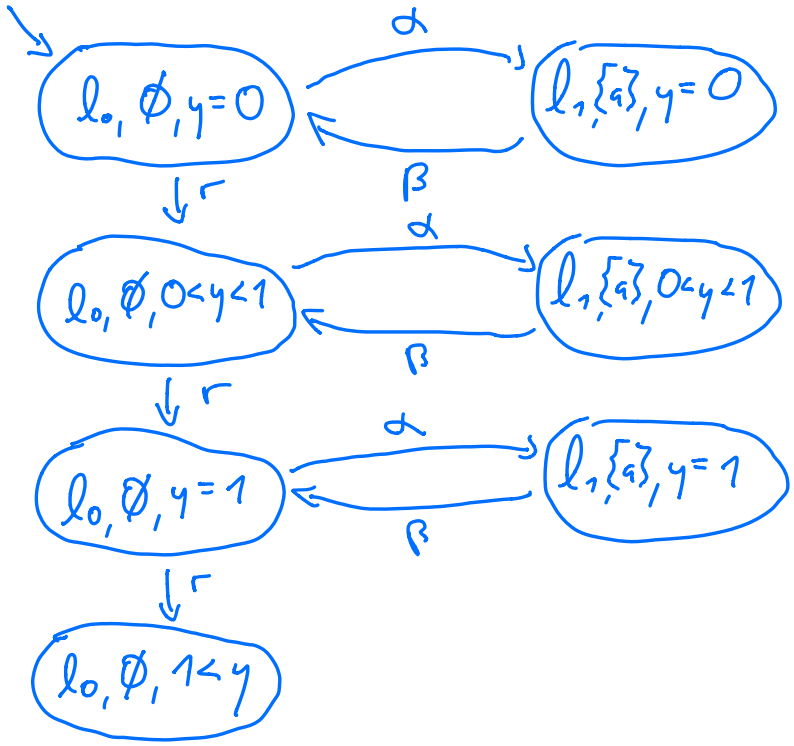


set of atomic propositions in a trace

1. Construct the region graph $[\![\mathcal{T}]\!]_r$ for $\mathcal{T}$.
2. Negate φ.
3. Construct a Büchi automaton $\mathcal{B}_{\neg\varphi}$.
4. Construct $[\![\mathcal{T}]\!]_r \parallel \mathcal{B}_{\neg\varphi}$.
5. Search for reachable loops with accepting states in $[\![\mathcal{T}]\!]_r \parallel \mathcal{B}_{\neg\varphi}$

Clock only increased in delay action, that's why invariant above always holds

1.)

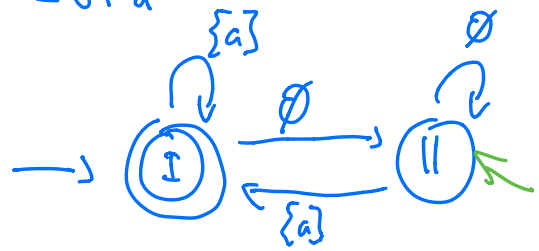


2.) Why negating phi?

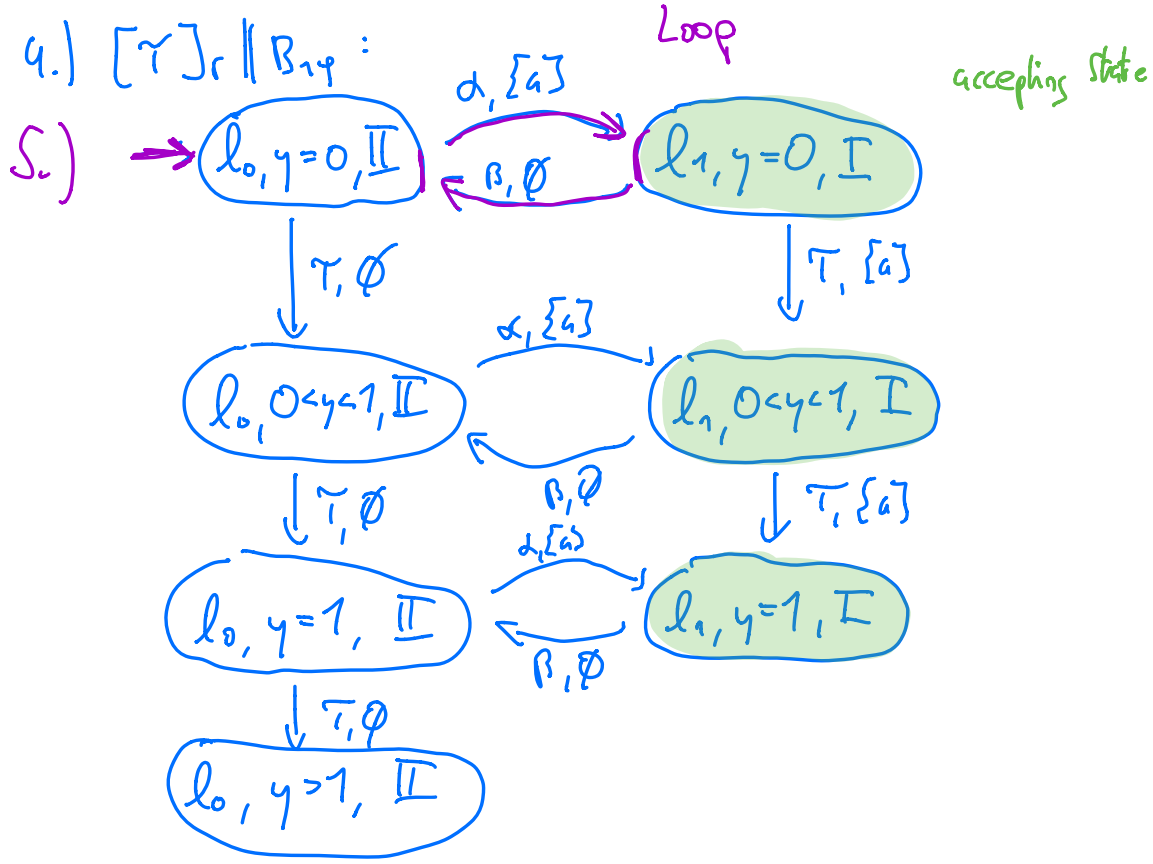
- Check if the formula holds
- composition of automata with negation, if reaching accepting state, it does not fulfill

$$\neg\varphi = \neg F(G \neg a)$$
$$\equiv G \neg G \neg a$$
$$\equiv GF(\neg a)$$
$$\equiv \delta F a$$

3.)



4.) $[\Upsilon]_r \| B_{\neg\varphi}$:



$\Rightarrow$ Loop $\rightsquigarrow$ ph: φ does not hold on Υ_0

(If no restrict ourselves to traces with infinitely many τ_1
$\alpha \rightarrow \tau \rightarrow \beta \rightarrow \tau \rightarrow \dots$
φ would hold)

3 parallel reliability: works if any part works

serial reliability: works if all parts work

$F(\boxed{01}) = P(0) \cdot F(1) = (1-0{,}1) \cdot (1-0{,}7) = 0{,}06$

$F(\boxed{012}) = F(\boxed{01}) \cdot F(2) = 0{,}06 \cdot 0{,}1 = 0{,}006$

$F(\boxed{345}) = 0{,}030625$

$R(\boxed{345}) = 1 - F(\boxed{345}) = 0{,}969375$

$R(\boxed{012}) = 0{,}994$ $\qquad$ $R(\boxed{012345}) = 0{,}96355875$

Cutsets $= \{\{0,1,2\}, \{3,4,5\}\}$

$R(+) \geq 1 - (0{,}054 + 0{,}0306\ldots)$

$= 0{,}915375$

good approximation

Better Algorithm:

- In general similar computational effort bc. you have to find minimal cut sets

Is better to compute it precisely right away.

Term path has to be finite

[4] Multiple guess solution:

Intuition:

Basic Paths:

① @pre
accu := 0
i := 0
@L

② @L
assume idx
accu := accu + s[i]
assume accu div len ≥ 200
@post

③ @L
assume idx
accu := accu + s[i]
assume accu div len < 200
@L

④ @L
assume idx
avg = accu div len
r = (avg ≥ 200)
@post

rc: @ φ_{sn}
: ; show that $\varphi \rightarrow wp(\psi, s_{mi}, \ldots s_n)$
@ ψ_{sn}

Example:

Example

$@L\ i \geq 0 \wedge accu = \sum_{j=0}^{i} s[j] \wedge \frac{accu}{len} < 200$

Ex Path ①

1. Calculate weakest precondition of loop invariant
   1. call wp(L, accu=0, i=0)
   2. show pre → ?

wp(L, accu=0; i=0)

$= 0 \geq 0 \wedge 0 = \sum_{j=0}^{0} s[j] \wedge \frac{0}{len} < 200$

$\equiv \top$