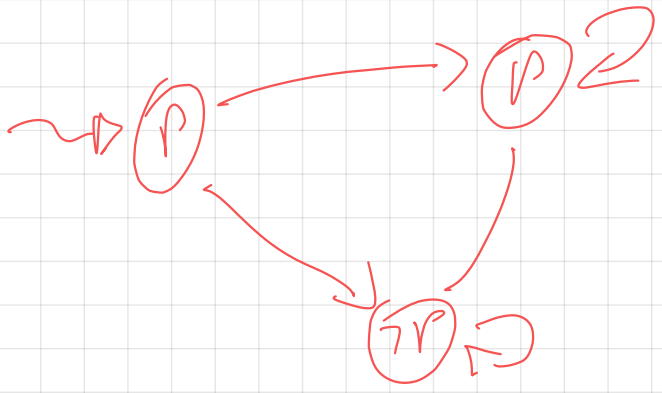
LTL Model Checking

TS γ $\models$ LTL ϕ

state & transition graph

ϕ: interpreted over infinite traces

$\gamma \Rightarrow \{t \mid t$ is an infinite trace of $\gamma\}$



$\{ r\ r\ r\ r\ r \cdots$
$\cdots$
$r\ r \cdots r\ \neg r\ \neg r\ \neg r \cdots$ (any finite)

$\mathcal{L}(\gamma) = \{t \mid t$ is a finite run of $\gamma\}$

$\mathcal{L}(\phi) = \{t \mid t \models \phi\}$

$\gamma \models \phi$ it means that:

$\mathcal{L}(\gamma) \subseteq \mathcal{L}(\phi)$

$\forall\, t$ of γ it is the case that $t \models \phi$

Suppose that $\mathcal{L}(\gamma)$ and $\mathcal{L}(\phi)$ are regular languages (RE / NFA / DFA)

$\gamma \rightsquigarrow A_\gamma$ $\quad$ $\phi \rightsquigarrow A_\phi$

$\mathcal{L}(\gamma) = \mathcal{L}(A_\gamma)$ $\quad$ $\mathcal{L}(\phi) = \mathcal{L}(A_\phi)$

$$\mathcal{L}(A_\gamma) \subseteq \mathcal{L}(A_\phi)$$

$$\forall\, t \in \mathcal{L}(A_\gamma) \Rightarrow t \in \mathcal{L}(A_\phi)$$

$$\neg\exists\, t \in \mathcal{L}(A_\gamma) \wedge t \notin \mathcal{L}(A_\phi)$$

$$\neg\exists\, t \in \mathcal{L}(A_\gamma \times \overline{A_\phi})$$

suppose regular

$\alpha \Rightarrow \beta$

$\neg(\neg\alpha \vee \beta)$

$\alpha \wedge \neg\beta$

$\wedge$ and $\overline{A_\phi}$ complement of A_ϕ

deterministic finite state automata

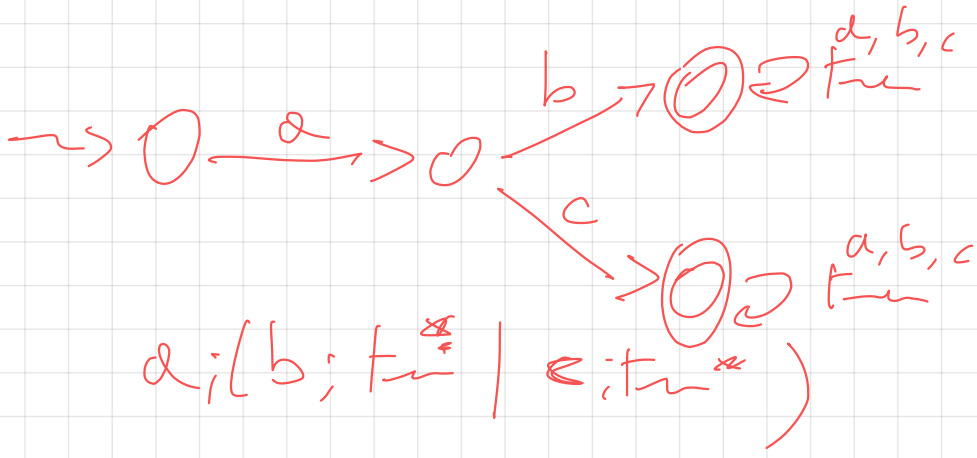
DFA

implementable machines

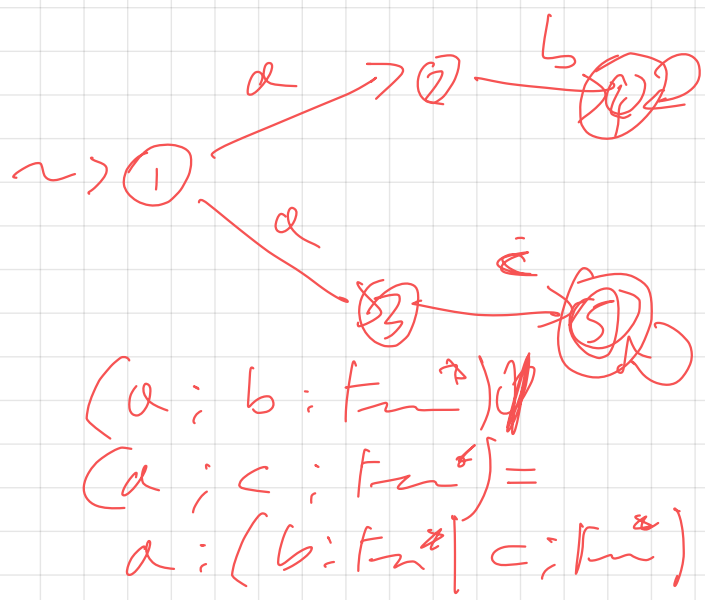
nondeterministic finite state automata

NFA

NOT implementable !

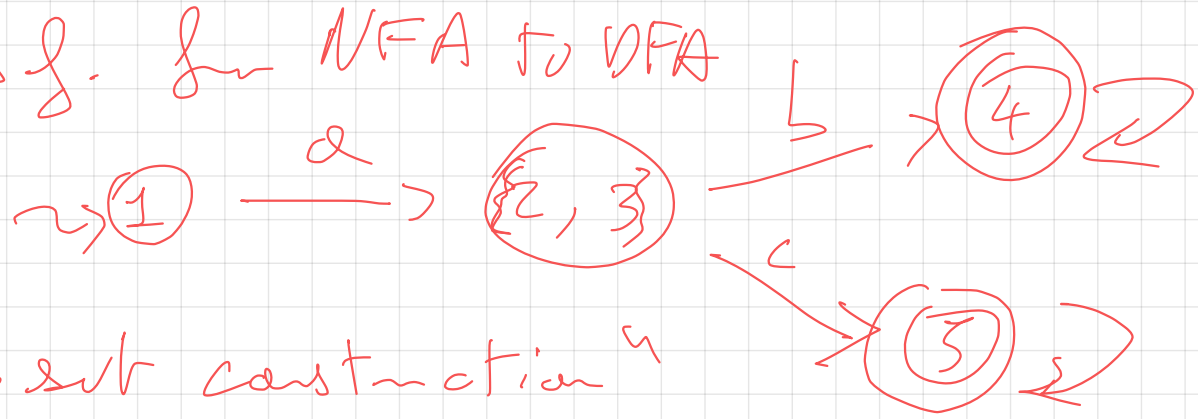


=



Th: $\forall$ NFA $\exists$ DFA s.t.

$$\mathcal{L}(NFA) = \mathcal{L}(DFA)\ !$$



"subset construction"

exp

but good (from comp. point of view) in practice

DFA $A_{\mathcal{L}_1}$

DFA $A_{\mathcal{L}_2}$ $\Rightarrow$ $A_{\mathcal{L}_1} \wedge A_{\mathcal{L}_1}$ poly

$A_{\mathcal{L}_1} \vee A_{\mathcal{L}_2}$ poly

$\neg \overline{A_{\mathcal{L}_1}}$ complem poly

closed under boolean operations

NFA $A_{\mathcal{N}_1}$

NFA $A_{\mathcal{N}_2}$ $\Rightarrow$

$A_{\mathcal{N}_1} \wedge A_{\mathcal{N}_2}$ poly

$A_{\mathcal{N}_1} \vee A_{\mathcal{N}_2}$ poly

~~$A_{\mathcal{N}_1}$~~ no complem.

closed under NFA operations

exp poly

$A_{\mathcal{N}_1} \rightsquigarrow A_{\mathcal{L}_1} \rightsquigarrow \overrightarrow{\overline{A_{\mathcal{L}_1}}}$

$\mathcal{L}(A_{\mathcal{N}_1}) = \Sigma^* - \mathcal{L}(A_{\mathcal{L}_1})$

alphabet

Th: NFA $\rightsquigarrow$ DFA very important

NFA can be checked for

emptiness / non-emptiness

check : $\text{If } \mathcal{L}(A_n) \overset{\neq}{=} \begin{matrix} \not\emptyset \text{ non-empty} \\ \not\emptyset \text{ empty} \end{matrix}$? $\in$ PSPACE

NLOGSPACE

Requires reachability on graph (the graph of the NFA)

checks for reachability $\boxed{\exists n \in \mathbb{N}.\ \text{Find } V <-> \mathbb{Z}}$

$$\mathcal{L}(\gamma) \subseteq \mathcal{L}(\phi)$$

$$\mathcal{L}(A_\gamma) \subseteq \mathcal{L}(A_\phi) \qquad \forall \Gamma.\ \Gamma \in \mathcal{L}(A_\gamma) \Rightarrow \Gamma \in \mathcal{L}(A_\phi)$$

$$\mathcal{L}(A_\gamma) \cap \overline{\mathcal{L}(A_\phi)} = \emptyset \qquad \Rightarrow \exists \Gamma.\ \Gamma \in \mathcal{L}(A_\gamma) \wedge \Gamma \notin \mathcal{L}(A_\phi)$$

$$\mathcal{L}(A_\gamma \wedge \overline{A_\phi}) = \emptyset$$

($\wedge$: poly; $\overline{\cdot}$: exp; $= \emptyset$: expspace)

But in fact we cannot use regular languages / Automata!

Because our traces are infinite

But we can use ω-regular languages

- Reg. Lang. $\mathcal{L}$: $\mathcal{L} \subseteq \Sigma^*$ (alphabet)
- ω-reg Lang $\mathcal{L}$: $\mathcal{L} \subseteq \Sigma^\omega$ ← is the first infinitary!

- Reg Lang $\mathcal{L}$: $\mathcal{L} = \mathcal{L}(A)$ ← DFA / NFA
- ω-reg Lang $\mathcal{L}$: $\mathcal{L} = \mathcal{L}(A)$ ← Nondeterministic Büchi automata NBA

alphabet, finite set of states, initial, transition rel/fun:

$$A = (\Sigma, S, S_0, tr, F)$$

& final states

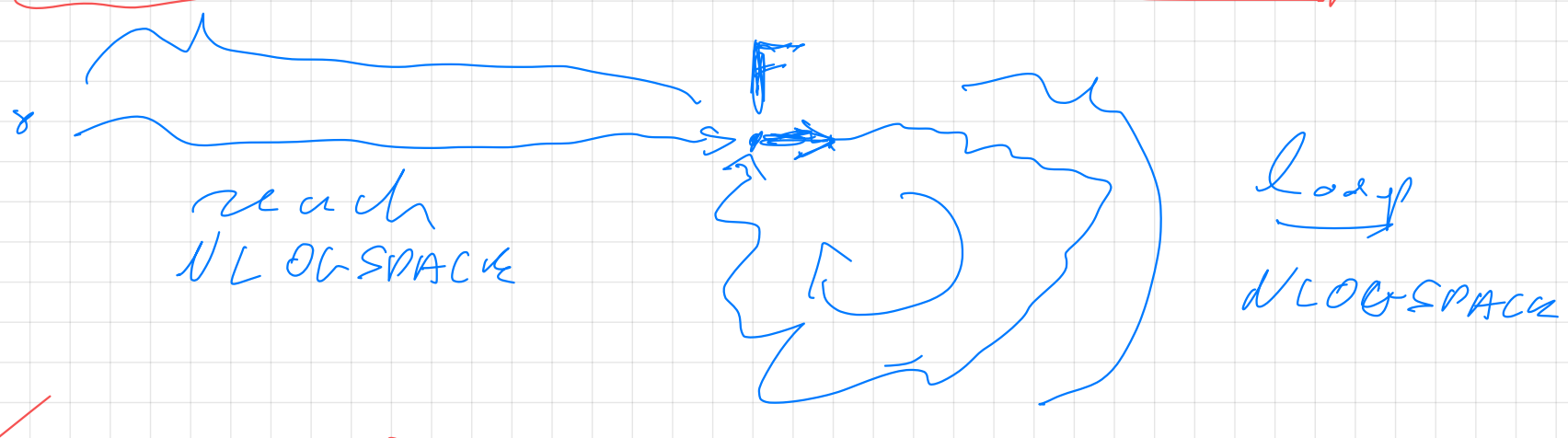
- Σ alphabet (is prop. interpretation for CTL)
- S finite set of states
- S_0 finite set of initial states $S_0 \subseteq S$
- F finite set of ~~final~~ accepting states $F \subseteq S$
- $tr : S \times A \to 2^S$ as function, or $S \times A \times S$ as relation

returns many values

Accepting condition:

- t reaches $s_f \in F$ as NFA
- end
- t loops over s_f:

"go to F infinitely often"



~~Th~~ NBA $\not\equiv$ DBA

it can be shown that DBA are less expressive than NBA.

NBA are closed for $\wedge$, $\vee$ but not for $\neg$

Th: NBA $\overset{\text{exp}}{\Leftrightarrow}$ DPA

extime alg. | bad alg.

parity

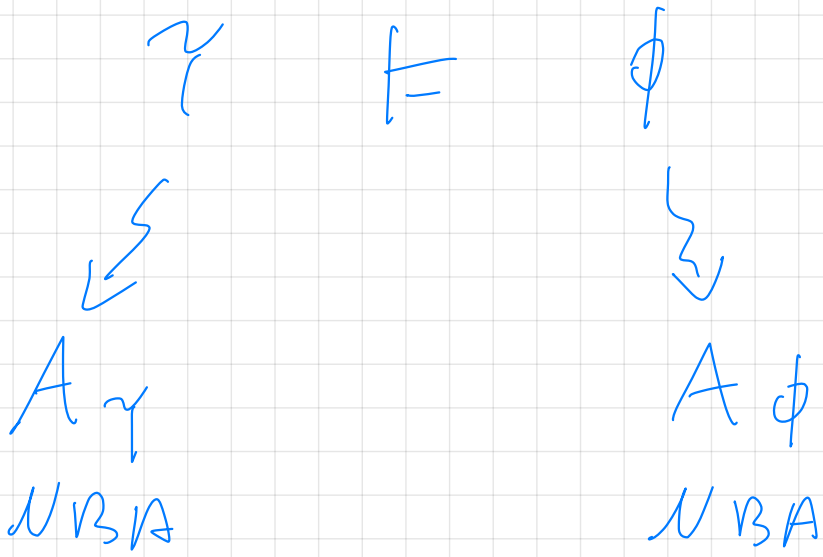
in practice too difficult to scale

Safra construction: very difficult

Checking for emptiness of Büchi automata is easy "gain reachability"
"find F on a loop" NLOGSPACE
easy!

$$\nu X.\ \mu Y.\ \left((F \wedge \langle\!\rangle X) \vee \langle\!\rangle Y\right)$$

μ-calc formula to check for "gain reachability"



$$\mathcal{L}(A_\gamma) \subseteq \mathcal{L}(A_\phi)$$

$$\mathcal{L}(A_\gamma \cap \overline{A_\phi}) \overset{\text{check}}{=} \emptyset$$

this is too different Vs implement in a scalable way

$A_\phi \rightsquigarrow \overline{A_\phi}$ too difficult

$\phi \rightsquigarrow \neg\phi$ easier!

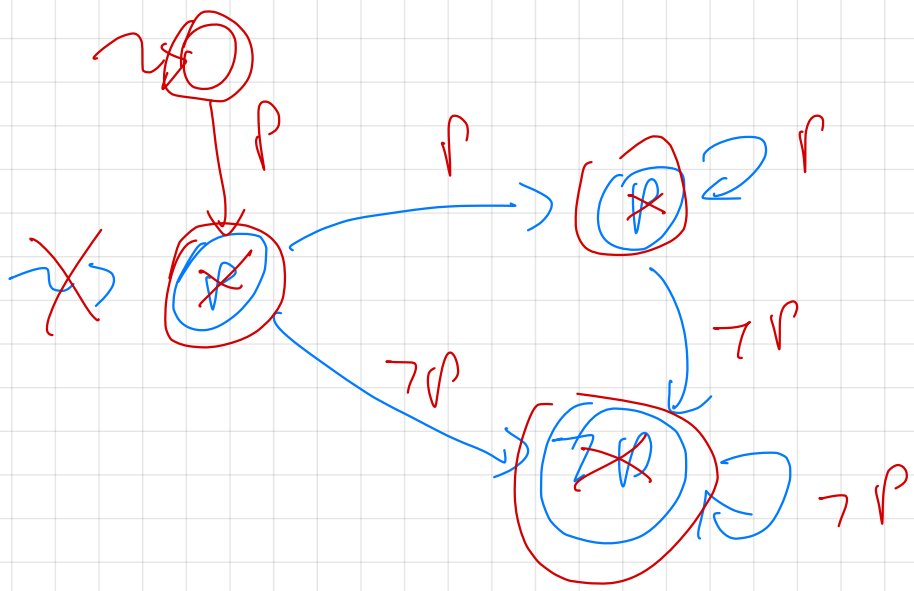
$$A_{\neg\phi} = \overline{A_\phi}$$

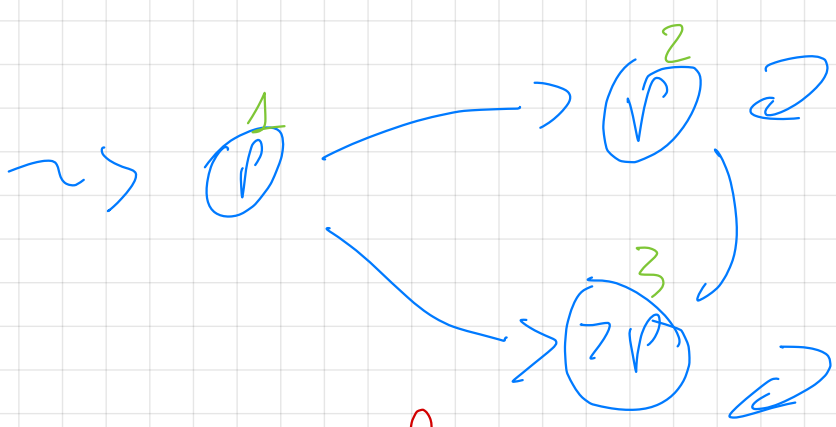
$$\mathcal{L}(A_\gamma \cap A_{\neg\phi}) \overset{\text{check}}{=} \emptyset$$

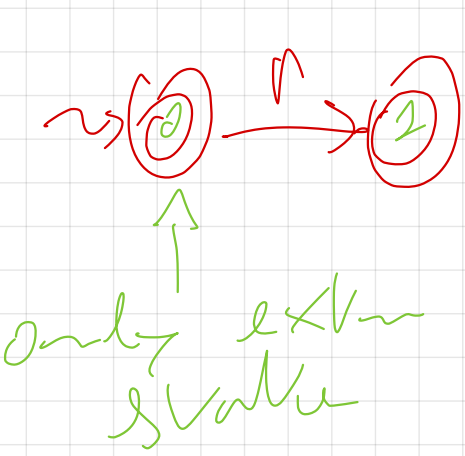
polytime polytime

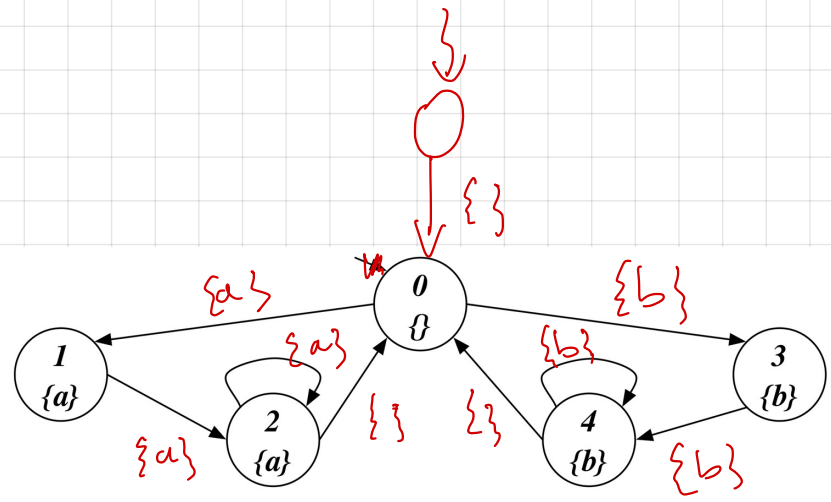
γ $\rightsquigarrow$ A_γ

(TS) (NBA)









To get A_γ from γ

- add extra dummy initial state
- put labelling on state to incoming transition
- Consider as accepting all states.

Th: $|A_\gamma| \approx |\gamma|$

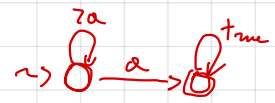
$\neg\phi$ (LTL) — EXP — $A_{\neg\phi}$ (NBA)

There are nice (also online) tools to get the NBA from an LTL formula

- SPOT
- LTL2BA

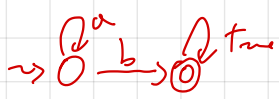
Some simple automata

$\Diamond a$



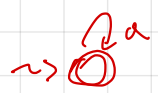
¬a ¬a -- ¬a a true true ...

$a \,\mathcal{U}\, b$

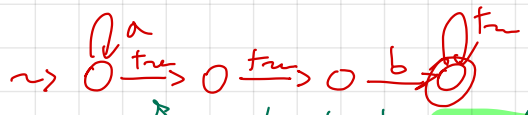


a a -- a b true true ...

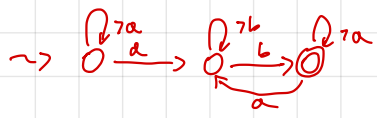
$\Box a$



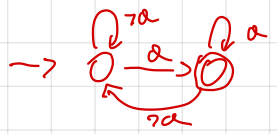
$a \,\mathcal{W}\, b$



$\Box(a \rightarrow \Diamond b)$



$\Box\Diamond a$



$\Diamond\Box a$

$\gamma \rightsquigarrow A_\gamma$

$\neg\phi \rightsquigarrow A_{\neg\phi}$

Product

$A_\gamma \wedge A_{\neg\phi}$

$A_\gamma \times A_{\neg\phi}$

every state is accepting!

$A_\gamma = (\Sigma, S_\gamma, S_{0\gamma}, tr_\gamma, F_\gamma)$

$A_{\neg\phi} = (\Sigma, S_{\neg\phi}, S_{0\neg\phi}, tr_{\neg\phi}, F_{\neg\phi})$

$A_\gamma \times A_{\neg\phi} = (\Sigma, S, S_0, tr, F)$

- Σ is the alphabet of both A_γ and $A_{\neg\phi}$
- $S = S_\gamma \times S_{\neg\phi}$ $\quad (s_\gamma, s_{\neg\phi}) \in S \Rightarrow s_\gamma \in S_\gamma$ and $s_{\neg\phi} \in S_{\neg\phi}$
- $S_0 = S_{0\gamma} \times S_{0\neg\phi}$ $\quad$ both automata start from initial states
- $F = S_\gamma \times F_{\neg\phi}$ $\quad$ check only $A_{\neg\phi}$ final.

  S_γ !

- $tr : S \times \Sigma \to 2^S$

$$tr((s_\gamma, s_{\neg\phi}), a) = \{(s'_\gamma, s'_{\neg\phi}) \mid s'_\gamma \in tr_\gamma(s_\gamma, a) \wedge s'_{\neg\phi} \in tr_{\neg\phi}(s_{\neg\phi}, a)\}$$

Intuitively:

Run the two automata simultaneously

NBA is not empty iff

(one of its) initial states belongs to

the extension of the following

μ-calc formula:

fair reachability

$$\varphi : \nu X_0 . \mu Y_0 . \left(F \wedge \langle act \rangle X \vee \langle - \rangle Y \right)$$

$$S_0 \cap [\![\varphi]\!] \neq \emptyset$$

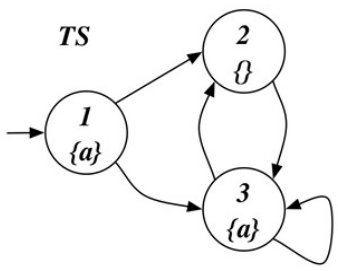
Observe: when evaluating $\forall \varphi$ over NBA

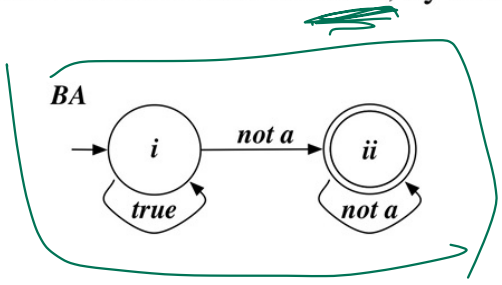
you may find states without successor!

μ-calc

(this never happens when we evaluate μ-calc over TS, since TS need to execute forever to generate infinite traces - "time never ends")

Exercise 5. Consider the transition system TS below. Model check the LTL formula $\Box\Diamond a$, by considering that the Büchi automaton BA for $\neg\Box\Diamond a$ (i.e., $\Diamond\Box\neg a$) is the one below:



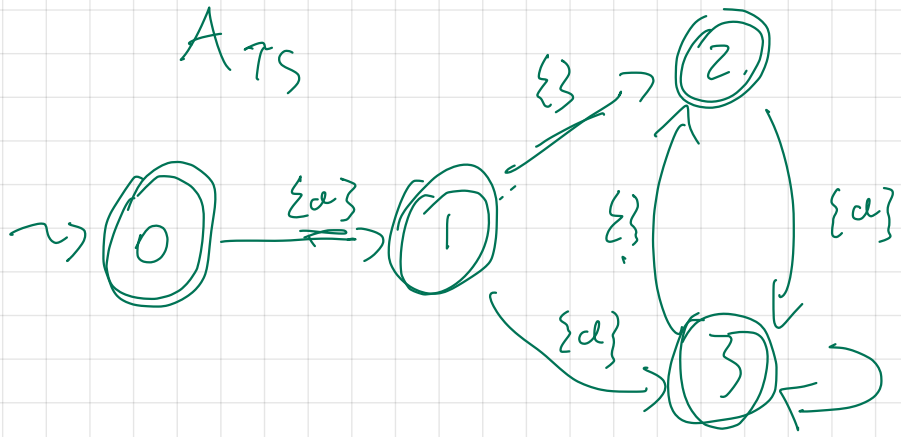


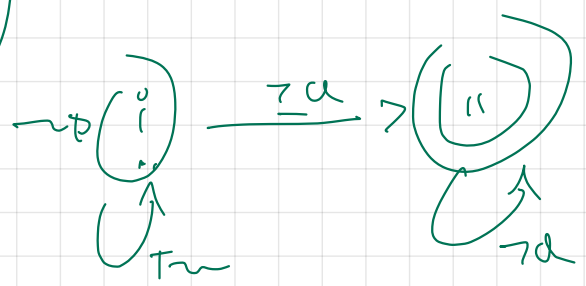
July 14, 2021

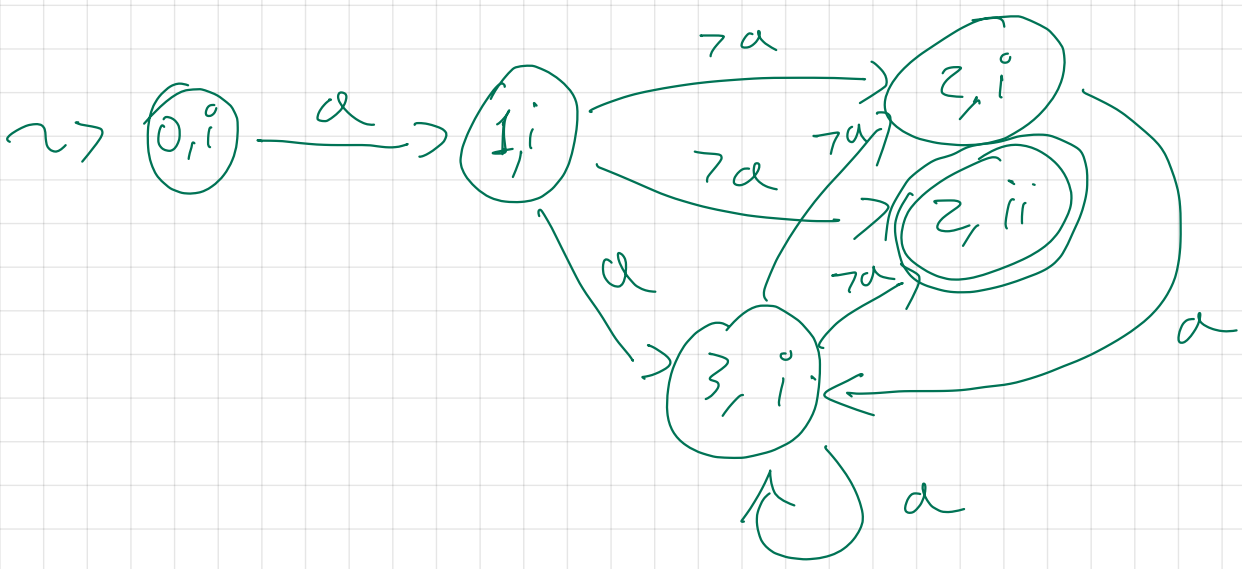
$TS \models \Box\Diamond a$

$\mathcal{L}(A_{TS} \cap A_{\neg\phi}) = \emptyset$

A_{TS}







$[\![\nu X.\ \mu Y((F \wedge \langle\!-\!\rangle X) \vee \langle\!-\!\rangle Y)]\!] = \emptyset$

$[\![X_0]\!] = \text{every thing}$

$[\![X_1]\!] = [\![\mu Y.((F \wedge \langle\!-\!\rangle X_0) \vee \langle\!-\!\rangle Y)]\!] = \emptyset$

$[\![Y_0]\!] = \emptyset$

$[\![Y_1]\!] = [\![(F \wedge \langle\!-\!\rangle X_0) \vee \langle\!-\!\rangle Y_0]\!] =$

$= [\![F]\!] \wedge Pre_{\exists}(-, [\![X_0]\!]) \vee Pre_{\exists}^{\phi}(-, [\![Y_0]\!]) = \phi$

$\{(2,ii)\}$ every thing $\neq \{(2,ii)\}$

$[\![X_2]\!] = [\![\mu Y.((F \wedge \langle\!-\!\rangle X_1) \vee \langle\!-\!\rangle Y)]\!] = \emptyset$

$[\![X_0]\!] = \phi$

$[\![Y_1]\!] = [\![(F \wedge \langle\!-\!\rangle X_1) \vee \langle\!-\!\rangle Y_0]\!] =$

$= [\![F]\!] \wedge Pre_{\exists}^{\emptyset}(-, [\![X_1]\!]) \vee Pre_{\exists}^{\emptyset}(-, [\![Y_0]\!]) = \emptyset$

$\{(2,ii)\}$

$(0,i) \notin [\![\varphi]\!] = \emptyset \quad \text{NO} \Rightarrow TS \models \Box\Diamond a$!