LTL model checking problem

LTL model checking problem

given: finite transition system $\mathcal{T}$ over ***AP***
(without terminal states)
LTL-formula φ over ***AP***

question: does $\mathcal{T} \models \varphi$ hold **?**

LTL model checking problem

given: finite transition system $\mathcal{T}$ over ***AP***
(without terminal states)
LTL-formula φ over ***AP***

question: does $\mathcal{T} \models \varphi$ hold **?**

basic idea: try to refute $\mathcal{T} \models \varphi$

LTL model checking problem

given: finite transition system $\mathcal{T}$ over AP
(without terminal states)
LTL-formula φ over AP

question: does $\mathcal{T} \models \varphi$ hold ?

basic idea: try to refute $\mathcal{T} \models \varphi$ by searching for a path π in $\mathcal{T}$ s.t.

$$\pi \not\models \varphi$$

LTL model checking problem

given: finite transition system $\mathcal{T}$ over ***AP***
(without terminal states)
LTL-formula φ over ***AP***

question: does $\mathcal{T} \models \varphi$ hold **?**

basic idea: try to refute $\mathcal{T} \models \varphi$ by searching for a path π in $\mathcal{T}$ s.t.

$$\pi \not\models \varphi, \text{ i.e., } \pi \models \neg\varphi$$

The LTL model checking problem

given: finite transition system $\mathcal{T}$ over ***AP***
LTL-formula φ over ***AP***

question: does $\mathcal{T} \models \varphi$ hold ?

1. construct an **NBA** $\mathcal{A}$ for ***Words***$(\neg\varphi)$

The LTL model checking problem

given: finite transition system $\mathcal{T}$ over AP
LTL-formula φ over AP

question: does $\mathcal{T} \models \varphi$ hold ?

1. construct an **NBA** $\mathcal{A}$ for $Words(\neg\varphi)$
2. search a path π in $\mathcal{T}$ with

$$trace(\pi) \in Words(\neg\varphi)$$

The LTL model checking problem

given: finite transition system $\mathcal{T}$ over AP
LTL-formula φ over AP

question: does $\mathcal{T} \models \varphi$ hold ?

1. construct an **NBA** $\mathcal{A}$ for $Words(\neg\varphi)$
2. search a path π in $\mathcal{T}$ with

$$trace(\pi) \in Words(\neg\varphi) = \mathcal{L}_\omega(\mathcal{A})$$

The LTL model checking problem

given: finite transition system $\mathcal{T}$ over AP
LTL-formula φ over AP

question: does $\mathcal{T} \models \varphi$ hold ?

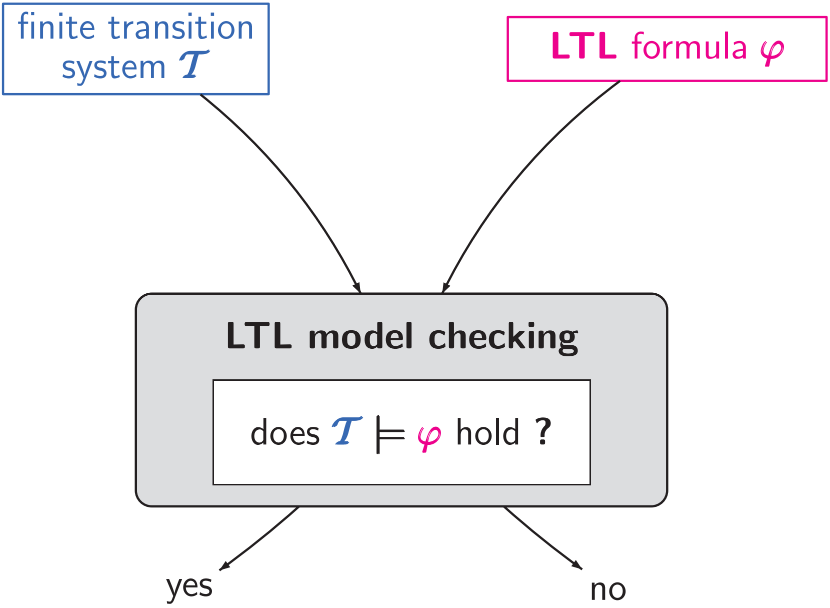
1. construct an **NBA** $\mathcal{A}$ for $Words(\neg\varphi)$
2. search a path π in $\mathcal{T}$ with

$$trace(\pi) \in Words(\neg\varphi) = \mathcal{L}_\omega(\mathcal{A})$$

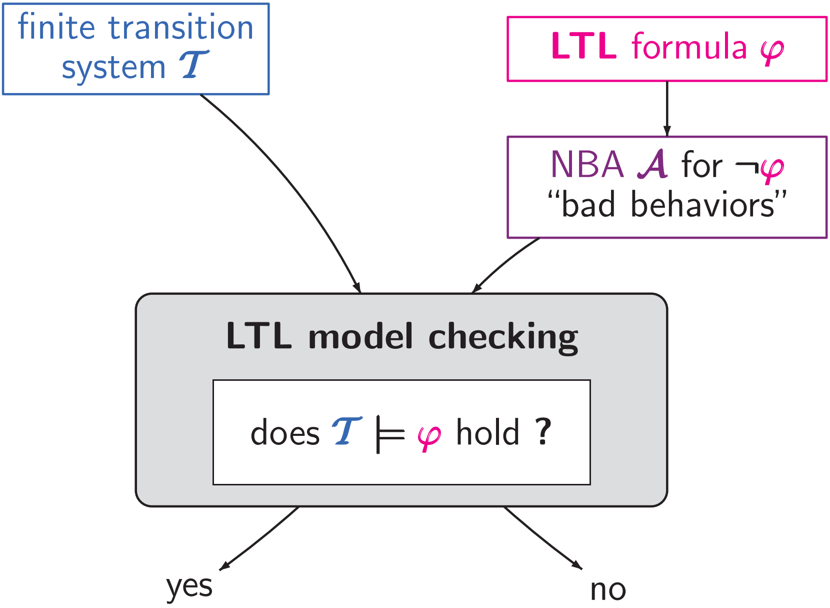
↑

construct the product-TS $\mathcal{T} \otimes \mathcal{A}$
search a path in the product that meets
the acceptance condition of $\mathcal{A}$

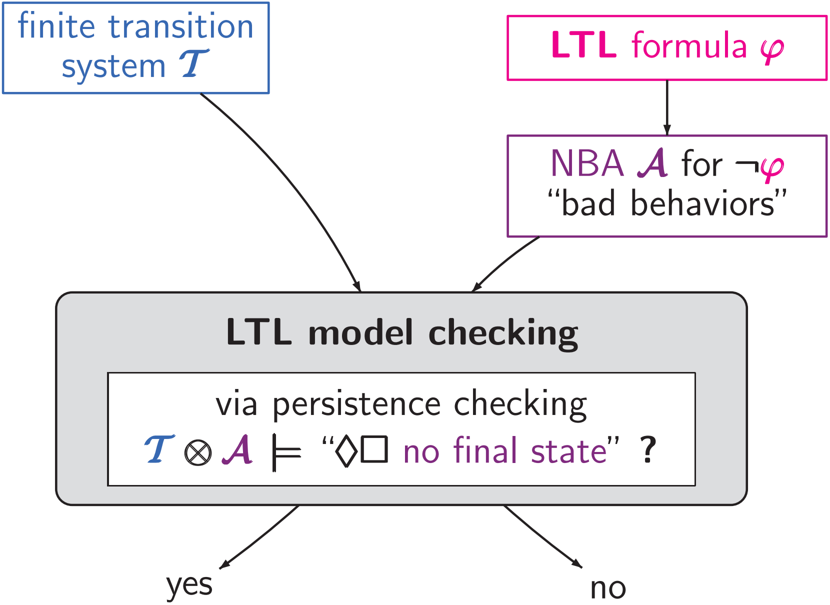
Automata-based LTL model checking



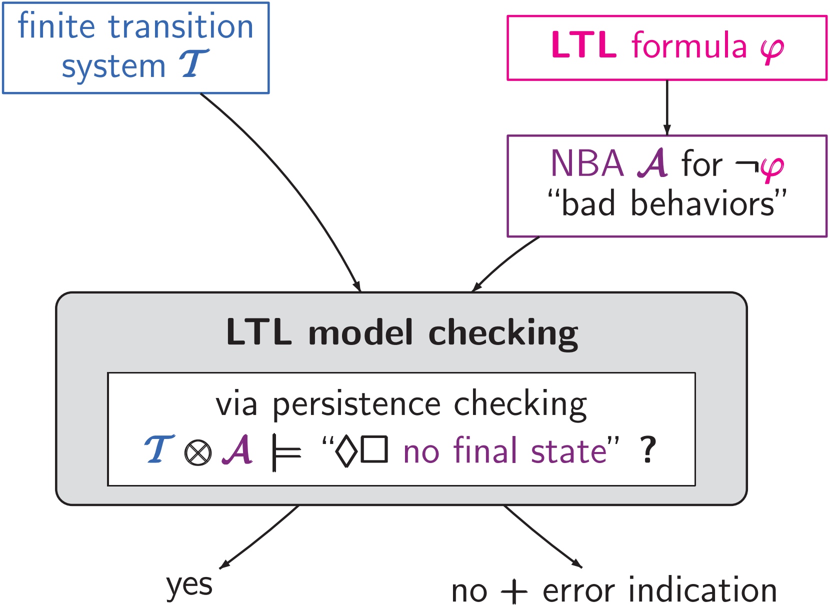
Automata-based LTL model checking



Automata-based LTL model checking



Automata-based LTL model checking



NBA $\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$

- Q finite set of states
- Σ alphabet
- $\delta : Q \times \Sigma \rightarrow 2^Q$ transition relation
- $Q_0 \subseteq Q$ set of initial states
- $F \subseteq Q$ set of final states, also called accept states

run for a word $A_0 A_1 A_2 \ldots \in \Sigma^\omega$:

state sequence $\pi = q_0 q_1 q_2 \ldots$ where $q_0 \in Q_0$
and $q_{i+1} \in \delta(q_i, A_i)$ for $i \geq 0$

run π is accepting if $\overset{\infty}{\exists} i \in \mathbb{N}.\ q_i \in F$

Recall: nondeterministic Büchi automata

NBA $\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$

- Q finite set of states
- Σ alphabet
- $\delta : Q \times \Sigma \to 2^Q$ transition relation
- $Q_0 \subseteq Q$ set of initial states
- $F \subseteq Q$ set of final states, also called accept states

accepted language $\mathcal{L}_\omega(\mathcal{A}) \subseteq \Sigma^\omega$ is given by:

$\mathcal{L}_\omega(\mathcal{A}) \stackrel{\text{def}}{=}$ set of infinite words over Σ that have an accepting run in $\mathcal{A}$

Recall: nondeterministic Büchi automata

NBA $\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$

- Q finite set of states
- Σ alphabet $\longleftarrow$ here: $\Sigma = 2^{AP}$
- $\delta : Q \times \Sigma \to 2^Q$ transition relation
- $Q_0 \subseteq Q$ set of initial states
- $F \subseteq Q$ set of final states, also called accept states

accepted language $\mathcal{L}_\omega(\mathcal{A}) \subseteq \Sigma^\omega$ is given by:

$\mathcal{L}_\omega(\mathcal{A}) \stackrel{\text{def}}{=}$ set of infinite words over Σ that have an accepting run in $\mathcal{A}$

From LTL to NBA

From LTL to NBA

For each **LTL** formula φ over AP there is an **NBA** $\mathcal{A}$ over the alphabet 2^{AP} such that

$$Words(\varphi) = \mathcal{L}_\omega(\mathcal{A})$$

From LTL to NBA

For each **LTL** formula φ over AP there is an **NBA** $\mathcal{A}$ over the alphabet 2^{AP} such that

- $Words(\varphi) = \mathcal{L}_\omega(\mathcal{A})$
- $size(\mathcal{A}) = \mathcal{O}\big(\exp(|\varphi|)\big)$

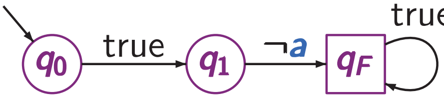
From LTL to NBA

For each **LTL** formula φ over AP there is an **NBA** $\mathcal{A}$ over the alphabet 2^{AP} such that

- $Words(\varphi) = \mathcal{L}_\omega(\mathcal{A})$
- $size(\mathcal{A}) = \mathcal{O}\big(\exp(|\varphi|)\big)$

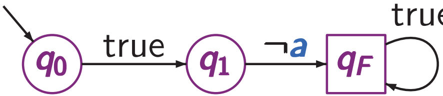
proof: ... later ...

NBA for LTL formulas



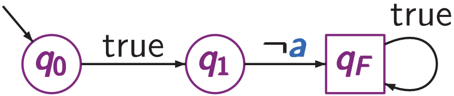
$\mathcal{L}_\omega(\mathcal{A}) =$ **?**

NBA for LTL formulas

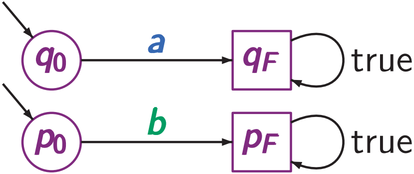


$$\mathcal{L}_\omega(\mathcal{A}) = \mathit{Words}(\bigcirc \neg a)$$

NBA for LTL formulas

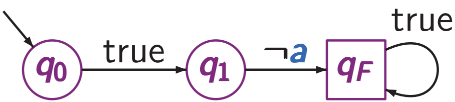


$\mathcal{L}_\omega(\mathcal{A}) = Words(\bigcirc \neg a)$

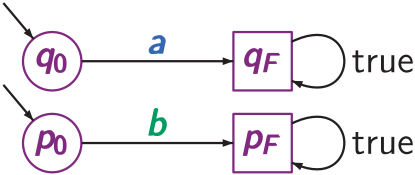


$\mathcal{L}_\omega(\mathcal{A}) = ?$

NBA for LTL formulas

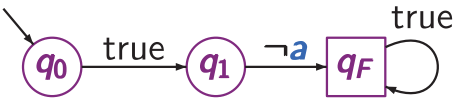


$$\mathcal{L}_\omega(\mathcal{A}) = Words(\bigcirc \neg a)$$

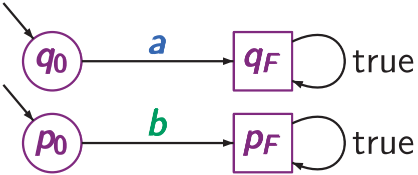


$$\mathcal{L}_\omega(\mathcal{A}) = Words(a \vee b)$$

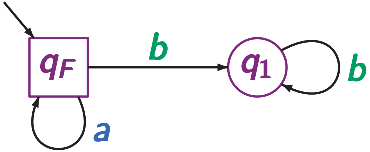
NBA for LTL formulas



$$\mathcal{L}_\omega(\mathcal{A}) = \mathit{Words}(\bigcirc \neg a)$$

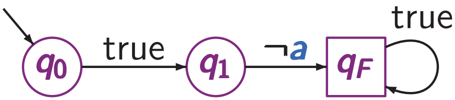


$$\mathcal{L}_\omega(\mathcal{A}) = \mathit{Words}(a \vee b)$$

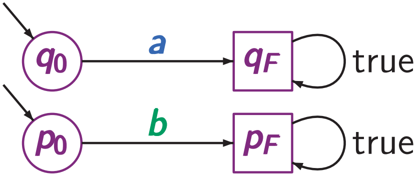


$$\mathcal{L}_\omega(\mathcal{A}) = \,?$$

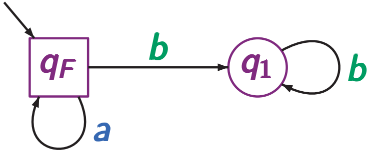
NBA for LTL formulas



$$\mathcal{L}_\omega(\mathcal{A}) = Words(\bigcirc \neg a)$$

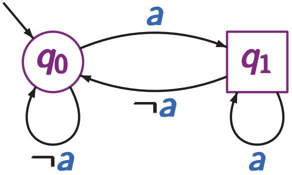


$$\mathcal{L}_\omega(\mathcal{A}) = Words(a \vee b)$$



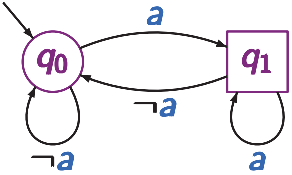
$$\mathcal{L}_\omega(\mathcal{A}) = Words(\Box a)$$

NBA for LTL formulas



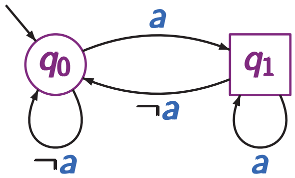
$$\mathcal{L}_\omega(\mathcal{A}) = \textbf{?}$$

NBA for LTL formulas

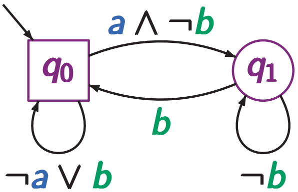


$$\mathcal{L}_\omega(\mathcal{A}) = Words(\Box\Diamond a)$$

NBA for LTL formulas

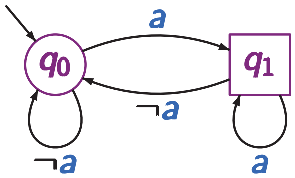


$\mathcal{L}_\omega(\mathcal{A}) = Words(\Box\Diamond a)$

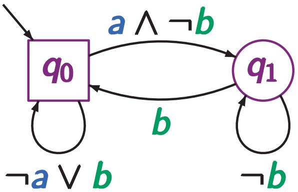


$\mathcal{L}_\omega(\mathcal{A}) = \,?$

NBA for LTL formulas

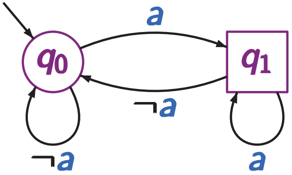


$\mathcal{L}_\omega(\mathcal{A}) = Words(\Box\Diamond a)$

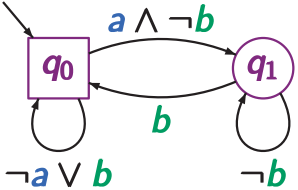


$\mathcal{L}_\omega(\mathcal{A}) = \,$?

e.g., $\varnothing\,\varnothing\,\varnothing\,\varnothing \ldots = \varnothing^\omega$ and $(\{a\}\,\{b\})^\omega$ are accepted by $\mathcal{A}$



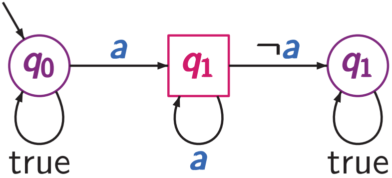
$$\mathcal{L}_\omega(\mathcal{A}) = \mathit{Words}(\Box\Diamond a)$$



$$\mathcal{L}_\omega(\mathcal{A}) = \mathit{Words}(\Box(a \rightarrow \Diamond b))$$

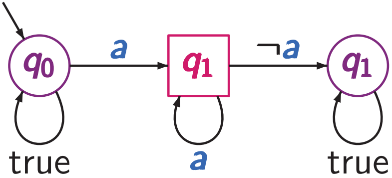
e.g., $\varnothing\,\varnothing\,\varnothing\,\varnothing \ldots = \varnothing^\omega$ and $(\{a\}\,\{b\})^\omega$ are accepted by $\mathcal{A}$

NBA for LTL formula



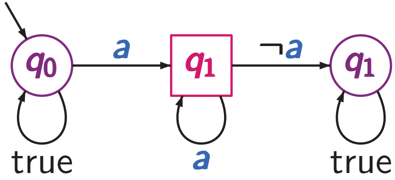
$$\mathcal{L}_\omega(\mathcal{A}) = \textbf{?}$$

NBA for LTL formula



$$\mathcal{L}_\omega(\mathcal{A}) = Words(\Diamond\Box a)$$

NBA for LTL formula



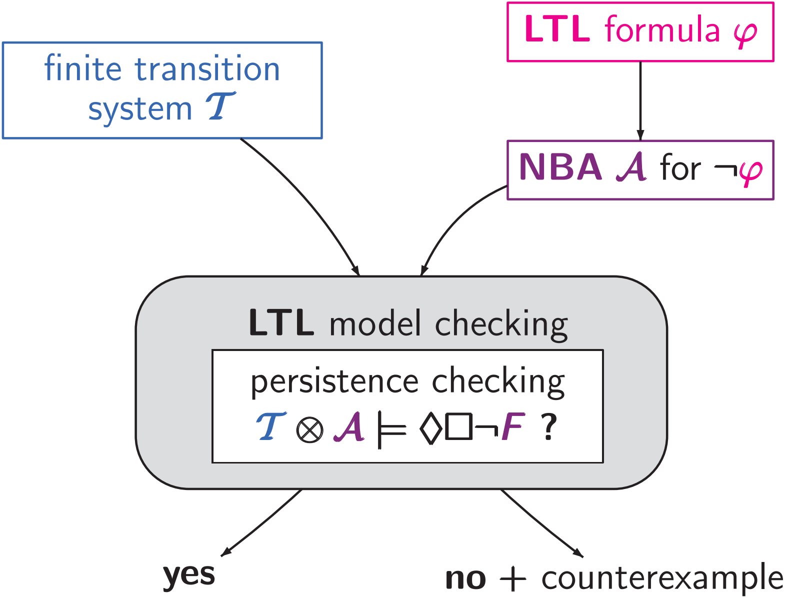
$$\mathcal{L}_\omega(\mathcal{A}) = Words(\Diamond\Box a)$$

possible runs for $\{a\}^\omega$

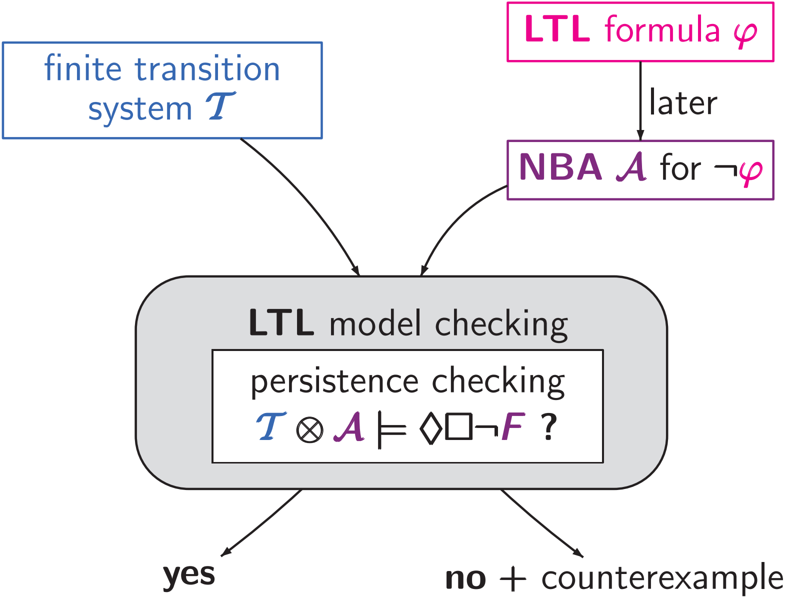
$q_0\ q_0\ q_0\ q_0\ q_0\ q_0\ \ldots$	not accepting
$q_0\ q_1\ q_1\ q_1\ q_1\ q_1\ \ldots$	accepting
$q_0\ q_0\ q_1\ q_1\ q_1\ q_1\ \ldots$	accepting
$q_0\ q_0\ q_0\ q_1\ q_1\ q_1\ \ldots$	accepting

$\vdots$

LTL model checking



LTL model checking



Recall: product transition system

$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$ TS without terminal states

$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$ NBA or NFA

non-blocking, $Q_0 \cap F = \varnothing$

Recall: product transition system

$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$ TS without terminal states

$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$ NBA or NFA

non-blocking, $Q_0 \cap F = \varnothing$

product-TS $\mathcal{T} \otimes \mathcal{A} \stackrel{\text{def}}{=} (S \times Q, Act, \rightarrow', S'_0, AP', L')$

Recall: product transition system

$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$ TS without terminal states

$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$ NBA or NFA

non-blocking, $Q_0 \cap F = \varnothing$

product-TS $\mathcal{T} \otimes \mathcal{A} \stackrel{\text{def}}{=} (S \times Q, Act, \rightarrow', S_0', AP', L')$

initial states: $S_0' = \{\langle s_0, q \rangle : s_0 \in S_0, q \in \delta(Q_0, L(s_0))\}$

labeling: $AP' = Q$, $L'(\langle s, q \rangle) = \{q\}$

$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$ TS without terminal states

$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$ NBA or NFA

non-blocking, $Q_0 \cap F = \varnothing$

product-TS $\mathcal{T} \otimes \mathcal{A} \stackrel{\text{def}}{=} (S \times Q, Act, \rightarrow', S'_0, AP', L')$

initial states: $S'_0 = \{\langle s_0, q \rangle : s_0 \in S_0, q \in \delta(Q_0, L(s_0))\}$

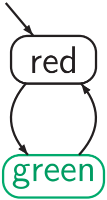
labeling: $AP' = Q$, $L'(\langle s, q \rangle) = \{q\}$

transition relation:

$$\frac{s \xrightarrow{\alpha} s' \;\wedge\; q' \in \delta(q, L(s'))}{\langle s, q \rangle \xrightarrow{\alpha}{}' \langle s', q' \rangle}$$

Example: LTL model checking

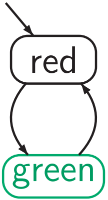
TS $\mathcal{T}$



LTL formula $\varphi = \Box\Diamond green$

Example: LTL model checking

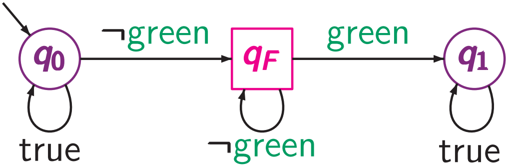
TS $\mathcal{T}$



LTL formula $\varphi = \Box\Diamond green$

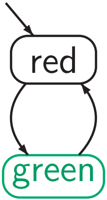
NBA $\mathcal{A}$ for the complement

$\neg\varphi \equiv \Diamond\Box\neg green$



Example: LTL model checking

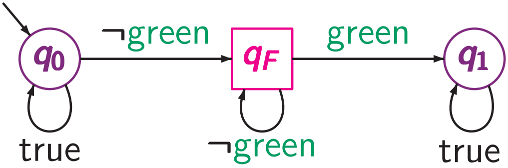
TS $\mathcal{T}$

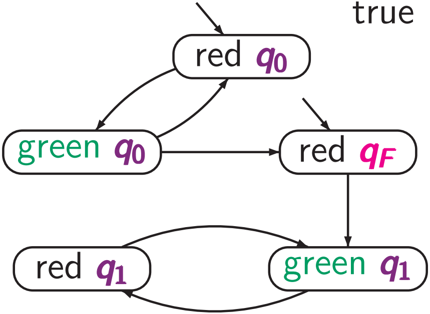


LTL formula $\varphi = \Box\Diamond$green

NBA $\mathcal{A}$ for the complement

$\neg\varphi \equiv \Diamond\Box\neg$green

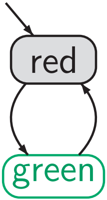




reachable fragment of the product TS $\mathcal{T} \otimes \mathcal{A}$

Example: LTL model checking

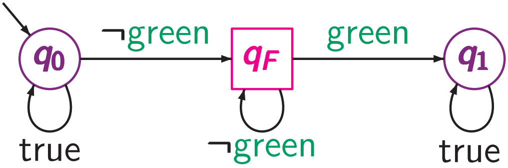
TS $\mathcal{T}$

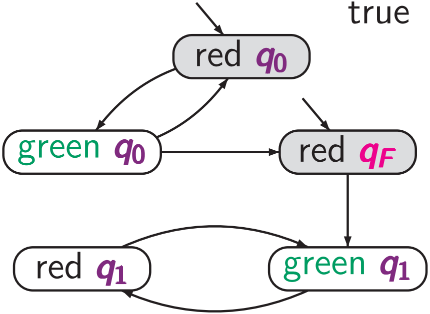


LTL formula $\varphi = \Box\Diamond \text{green}$

NBA $\mathcal{A}$ for the complement

$\neg\varphi \equiv \Diamond\Box\neg\text{green}$





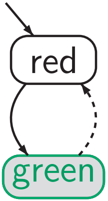
initial states:

$\langle \text{red}, q\rangle$ where

$$q \in \delta(q_0, L(\text{red})) = \delta(q_0, \varnothing) = \{q_0, q_F\}$$

Example: LTL model checking

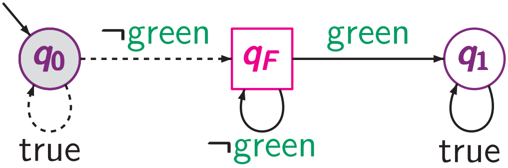
TS $\mathcal{T}$

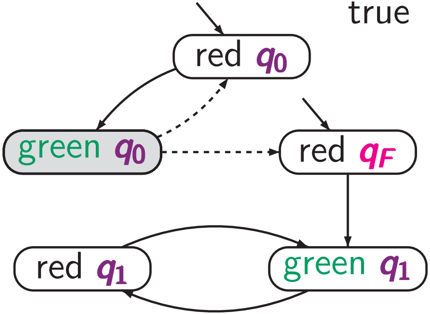


LTL formula $\varphi = \Box\Diamond green$

NBA $\mathcal{A}$ for the complement

$\neg\varphi \equiv \Diamond\Box\neg green$





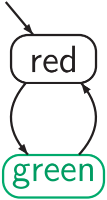
transition

$\langle green, q_0\rangle \rightarrow \langle red, q\rangle$

$$q \in \delta(q_0, L(red)) = \delta(q_0, \varnothing) = \{q_0, q_F\}$$

Example: LTL model checking

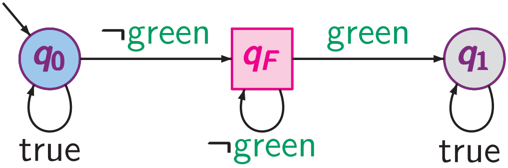
TS $\mathcal{T}$

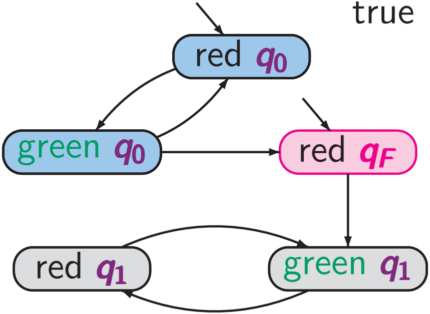


LTL formula $\varphi = \Box\Diamond green$

NBA $\mathcal{A}$ for the complement

$\neg\varphi \equiv \Diamond\Box\neg green$





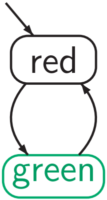
atomic propositions

$AP' = \{q_0, q_F, q_1\}$

obvious labeling function

Example: LTL model checking

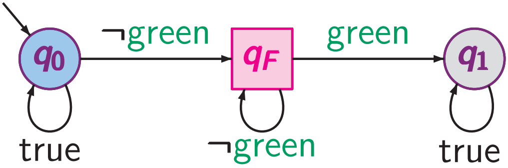
TS $\mathcal{T}$

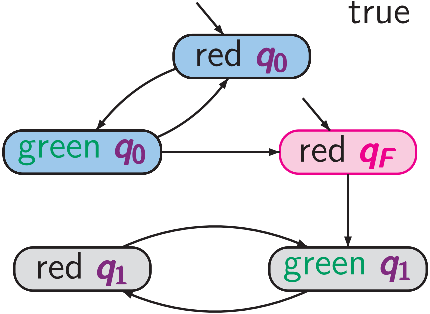


LTL formula $\varphi = \Box\Diamond \text{green}$

NBA $\mathcal{A}$ for the complement

$\neg\varphi \equiv \Diamond\Box\neg\text{green}$

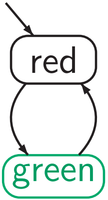




$\mathcal{T} \otimes \mathcal{A} \models \Diamond\Box\neg F$

Example: LTL model checking

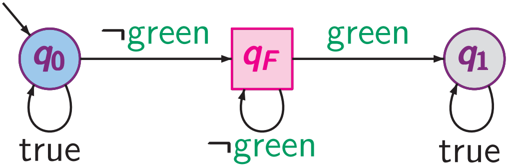
TS $\mathcal{T}$

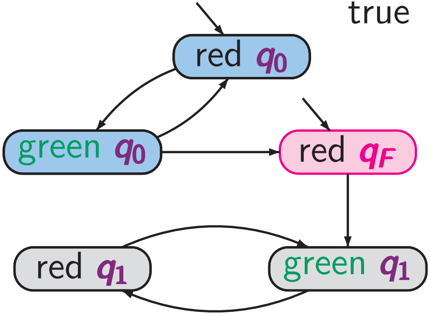


LTL formula $\varphi = \Box\Diamond \text{green}$

NBA $\mathcal{A}$ for the complement

$\neg\varphi \equiv \Diamond\Box\neg\text{green}$



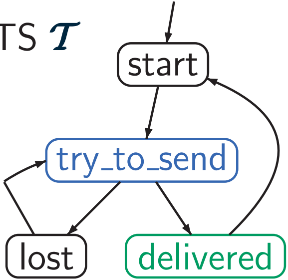


$\mathcal{T} \otimes \mathcal{A} \models \Diamond\Box\neg F$

hence: $\mathcal{T} \models \varphi$

Example: LTL model checking

TS $\mathcal{T}$

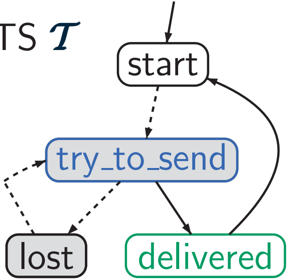


LTL formula $\varphi = \Box(try \rightarrow \Diamond del)$

"each (repeatedly) sent message will eventually be delivered"

Example: LTL model checking

TS $\mathcal{T}$



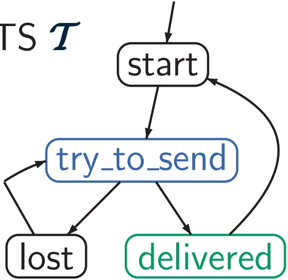
LTL formula $\varphi = \Box(\mathit{try} \rightarrow \Diamond \mathit{del})$

"each (repeatedly) sent message will eventually be delivered"

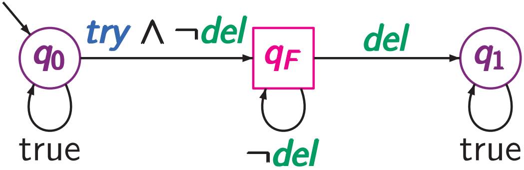
$\mathcal{T} \not\models \varphi$

Example: LTL model checking

TS $\mathcal{T}$



NBA $\mathcal{A}$ for $\neg\varphi \equiv \Diamond(try \wedge \Box\neg del)$

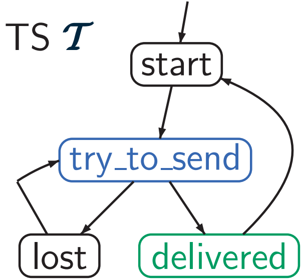


LTL formula $\varphi = \Box(try \rightarrow \Diamond del)$

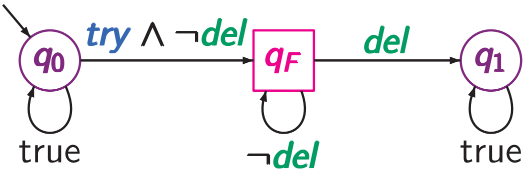
"each (repeatedly) sent message will eventually be delivered"

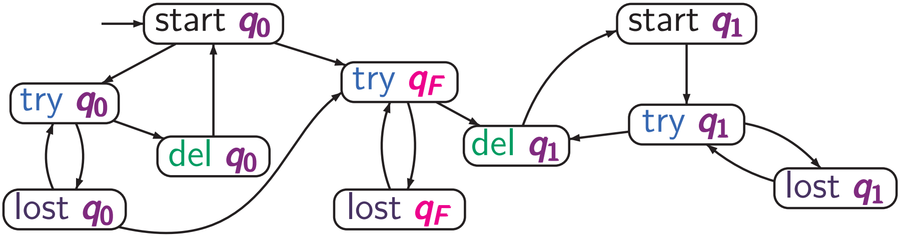
$\mathcal{T} \not\models \varphi$

Example: LTL model checking



NBA $\mathcal{A}$ for $\neg\varphi \equiv \Diamond(try \wedge \Box\neg del)$

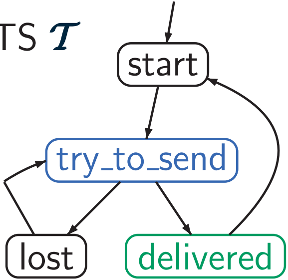




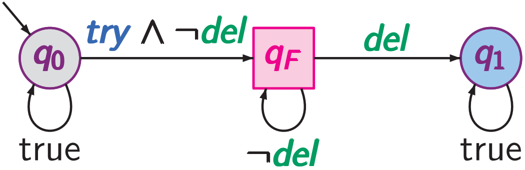
reachable fragment of the product-TS

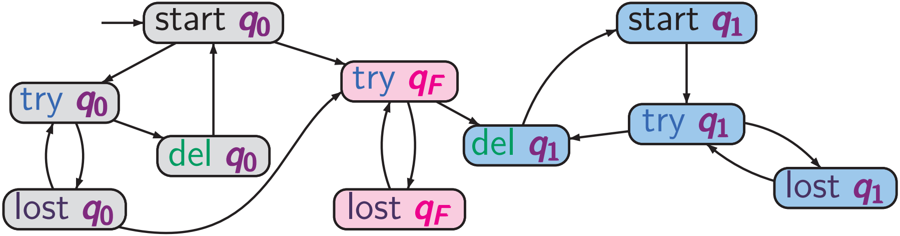
Example: LTL model checking

TS $\mathcal{T}$



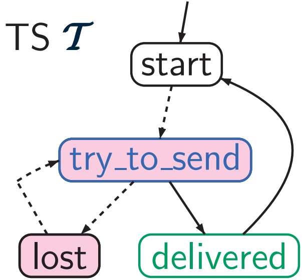
NBA $\mathcal{A}$ for $\neg\varphi \equiv \Diamond(try \wedge \Box\neg del)$



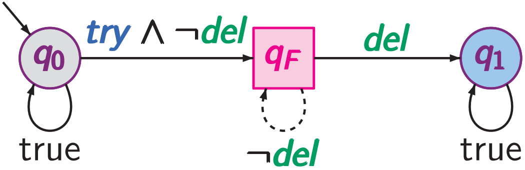


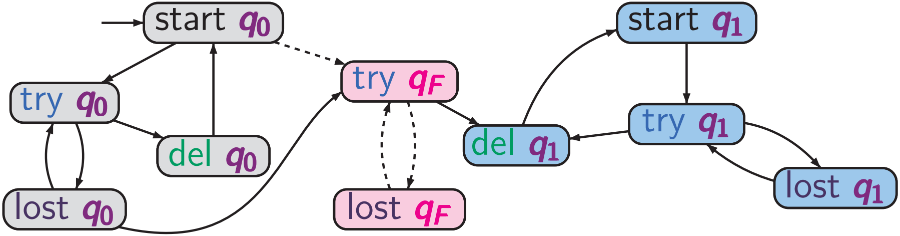
set of atomic propositions $AP' = \{q_0, q_1, q_F\}$

Example: LTL model checking



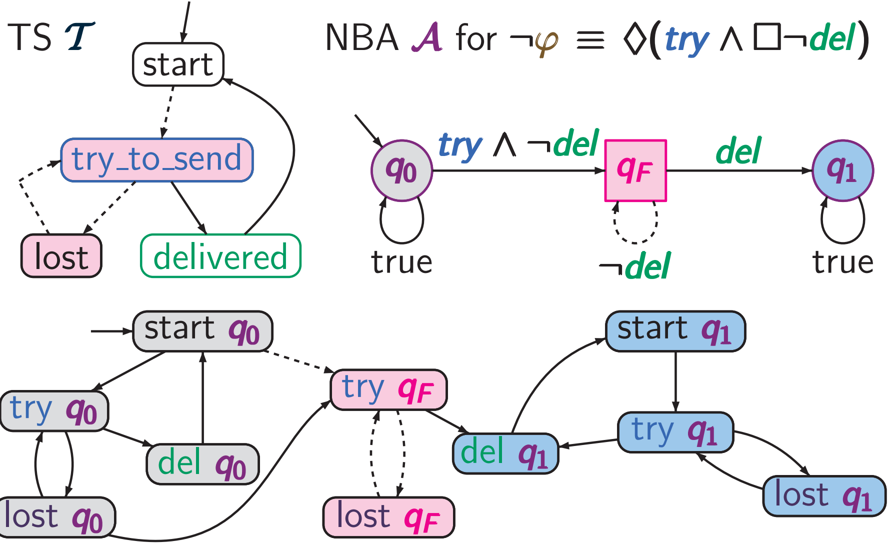
NBA $\mathcal{A}$ for $\neg\varphi \equiv \Diamond(try \wedge \Box\neg del)$





$$\mathcal{T} \otimes \mathcal{A} \not\models \Diamond\Box\neg F$$

Example: LTL model checking



$\mathcal{T} \otimes \mathcal{A} \not\models \Diamond\Box\neg F$ hence: $\mathcal{T} \not\models \varphi$

LTL model checking

given: finite TS $\mathcal{T}$, LTL-formula φ
question: does $\mathcal{T} \models \varphi$ hold **?**

given: finite TS $\mathcal{T}$, LTL-formula φ

question: does $\mathcal{T} \models \varphi$ hold **?**

construct an NBA $\mathcal{A}$ for $\neg\varphi$ and the product $\mathcal{T} \otimes \mathcal{A}$

check whether $\mathcal{T} \otimes \mathcal{A} \models \Diamond\Box\neg F$

given: finite TS $\mathcal{T}$, LTL-formula φ

question: does $\mathcal{T} \models \varphi$ hold ?

construct an NBA $\mathcal{A}$ for $\neg\varphi$ and the product $\mathcal{T} \otimes \mathcal{A}$

check whether $\mathcal{T} \otimes \mathcal{A} \models \Diamond\Box\neg F$ $\longleftarrow$ persistence checking nested **DFS**

given: finite TS $\mathcal{T}$, LTL-formula φ

question: does $\mathcal{T} \models \varphi$ hold **?**

construct an NBA $\mathcal{A}$ for $\neg\varphi$ and the product $\mathcal{T} \otimes \mathcal{A}$

check whether $\mathcal{T} \otimes \mathcal{A} \models \Diamond\Box\neg F$ ⟵ persistence checking nested **DFS**

IF $\mathcal{T} \otimes \mathcal{A} \models \Diamond\Box\neg F$

THEN return "**yes**"

ELSE compute a counterexample

$\langle s_0, p_0\rangle \ldots \langle s_n, p_n\rangle \ldots \langle s_n, p_n\rangle$

for $\mathcal{T} \otimes \mathcal{A}$ and $\Diamond\Box\neg F$

return "**no**" and $s_0 \ldots s_n \ldots s_n$

Complexity of LTL model checking

given: finite TS $\mathcal{T}$, LTL-formula φ

question: does $\mathcal{T} \models \varphi$ hold ?

~~construct an NBA $\mathcal{A}$~~ for $\neg\varphi$ and the product $\mathcal{T} \otimes \mathcal{A}$

check whether $\mathcal{T} \otimes \mathcal{A} \models \Diamond\Box\neg F$ ⟵ persistence checking nested **DFS**

IF $\mathcal{T} \otimes \mathcal{A} \models \Diamond\Box\neg F$

THEN return "**yes**"

ELSE compute a counterexample

$\langle s_0, p_0 \rangle \ldots \langle s_n, p_n \rangle \ldots \langle s_n, p_n \rangle$

for $\mathcal{T} \otimes \mathcal{A}$ and $\Diamond\Box\neg F$

return "**no**" and $s_0 \ldots s_n \ldots s_n$

time complexity: $\mathcal{O}(size(\mathcal{T}) \cdot size(\mathcal{A}))$