Temporal Logics

extend propositional or predicate logic by
temporal modalities, e.g.

$\Box\varphi$ "φ holds always", i.e., now and forever in the future

$\Diamond\varphi$ "φ holds now or eventually in the future"

here: two propositional temporal logics:

LTL: linear temporal logic

CTL: computation tree logic

Linear Temporal Logic (LTL)

syntax and semantics of LTL ←

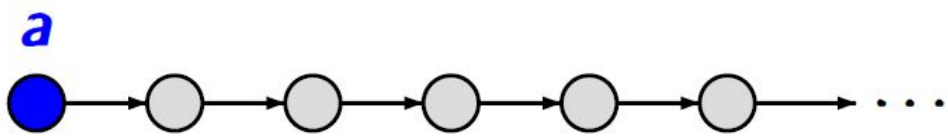
automata-based LTL model checking

Linear Temporal Logic (LTL)

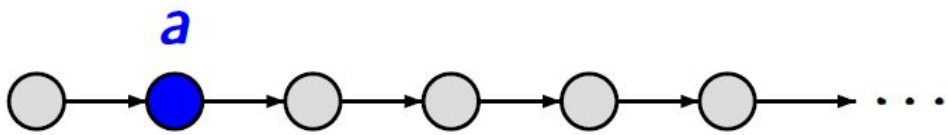
$$\varphi \;::=\; \textit{true} \;\big|\; a \;\big|\; \varphi_1 \wedge \varphi_2 \;\big|\; \neg\varphi \;\big|\; \bigcirc\varphi \;\big|\; \varphi_1 \,\mathsf{U}\, \varphi_2$$

where $a \in AP$ $\qquad \bigcirc \mathrel{\widehat{=}}$ next $\qquad \mathsf{U} \mathrel{\widehat{=}}$ until

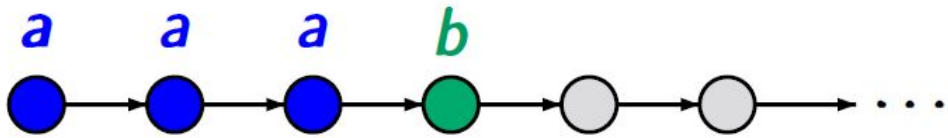
atomic proposition $a \in AP$



next operator $\bigcirc a$



until operator $a \,\mathsf{U}\, b$



Derived operators in LTL

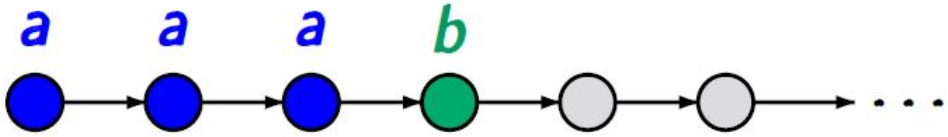
$$\varphi \;::=\; \mathit{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi_1 \,\mathsf{U}\, \varphi_2$$

derived operators:

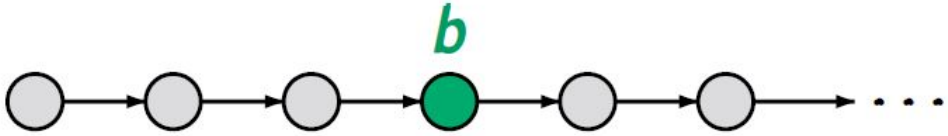
$\vee, \rightarrow, \ldots$ as usual

$\Diamond\varphi$	$\stackrel{\text{def}}{=}$	$\mathit{true}\,\mathsf{U}\,\varphi$	eventually
$\Box\varphi$	$\stackrel{\text{def}}{=}$	$\neg\Diamond\neg\varphi$	always

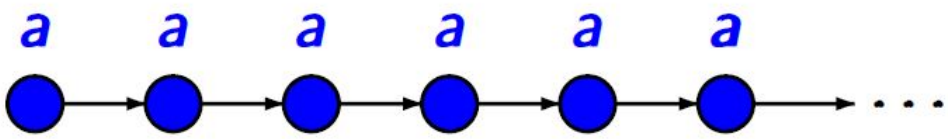
until operator
$a\,\mathsf{U}\,b$



eventually
$\Diamond b$

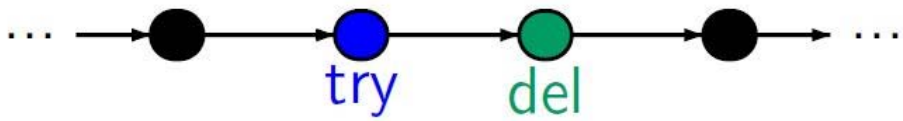


always
$\Box a$

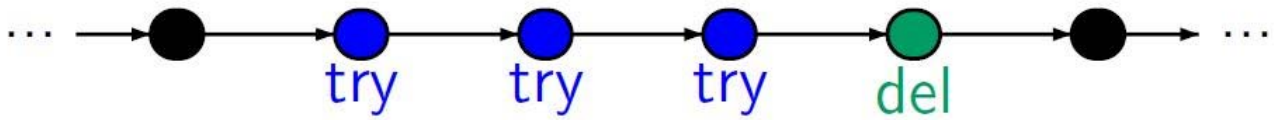


Next O , until U, eventually <>, and always []

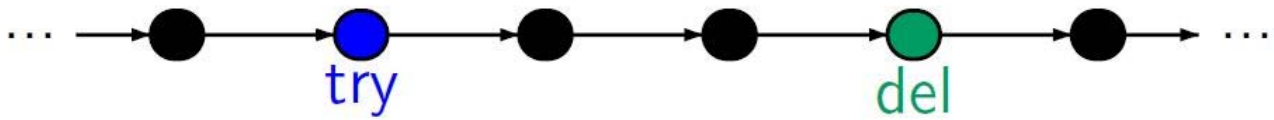
$\Box$ (try_to_send $\rightarrow$ $\bigcirc$ delivered)



$\Box$ (try_to_send $\rightarrow$ try_to_send **U** delivered)



$\Box$ (try_to_send $\rightarrow$ $\Diamond$ delivered)



Examples for LTL formulas

$$\varphi \ ::= \ \textit{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi_1 \,\mathbf{U}\, \varphi_2$$

eventually

$$\Diamond\varphi \stackrel{\text{def}}{=} \textit{true}\,\mathbf{U}\,\varphi$$

always

$$\Box\varphi \stackrel{\text{def}}{=} \neg\Diamond\neg\varphi$$

Examples for LTL formulas:

mutual exclusion: $\Box(\neg \mathit{crit}_1 \vee \neg \mathit{crit}_2)$

railroad-crossing: $\Box(\mathit{train_is_near} \rightarrow \mathit{gate_is_closed})$

progress property: $\Box(\mathit{request} \rightarrow \Diamond \mathit{response})$

traffic light: $\Box(\mathit{yellow} \vee \bigcirc\neg \mathit{red})$

Infinitely often and eventually forever

$$\varphi \;::=\; \mathit{true} \mid a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \bigcirc\varphi \mid \varphi_1 \,\mathbf{U}\, \varphi_2$$

eventually	$\Diamond\varphi$	$\stackrel{\text{def}}{=}\ \mathit{true}\,\mathbf{U}\,\varphi$
always	$\Box\varphi$	$\stackrel{\text{def}}{=}\ \neg\Diamond\neg\varphi$
infinitely often	$\Box\Diamond\varphi$	
eventually forever	$\Diamond\Box\varphi$	

e.g.,	unconditional fairness	$\Box\Diamond \mathit{crit}_i$
	strong fairness	$\Box\Diamond \mathit{wait}_i \rightarrow \Box\Diamond \mathit{crit}_i$
	weak fairness	$\Diamond\Box \mathit{wait}_i \rightarrow \Box\Diamond \mathit{crit}_i$

Semantics of LTL over infinite words

for $\sigma = A_0\, A_1\, A_2\, \ldots \in \left(2^{AP}\right)^{\omega}$:

$$\sigma \models \mathit{true}$$

$$\sigma \models a \quad \text{iff} \quad A_0 \models a \text{ ,i.e., } a \in A_0$$

$$\sigma \models \varphi_1 \wedge \varphi_2 \quad \text{iff} \quad \sigma \models \varphi_1 \text{ and } \sigma \models \varphi_2$$

$$\sigma \models \neg\varphi \quad \text{iff} \quad \sigma \not\models \varphi$$

$$\sigma \models \bigcirc\varphi \quad \text{iff} \quad \mathit{suffix}(\sigma, 1) = A_1\, A_2\, A_3\, \ldots \models \varphi$$

$$\sigma \models \varphi_1 \,\mathsf{U}\, \varphi_2 \quad \text{iff} \quad \text{there exists } j \geq 0 \text{ such that}$$

$$\mathit{suffix}(\sigma, j) = A_j\, A_{j+1}\, A_{j+2}\, \ldots \models \varphi_2 \quad \text{and}$$

$$\mathit{suffix}(\sigma, i) = A_i\, A_{i+1}\, A_{i+2}\, \ldots \models \varphi_1 \quad \text{for } 0 \leq i < j$$

LTL-semantics of derived operators <> and []

for $\sigma = A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega}$:

$$\vdots$$

$\sigma \models \varphi_1 \,\mathsf{U}\, \varphi_2$ iff there exists $j \geq 0$ such that

$A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi_2$ and

$A_i\, A_{i+1}\, A_{i+2} \ldots \models \varphi_1$ for $0 \leq i < j$

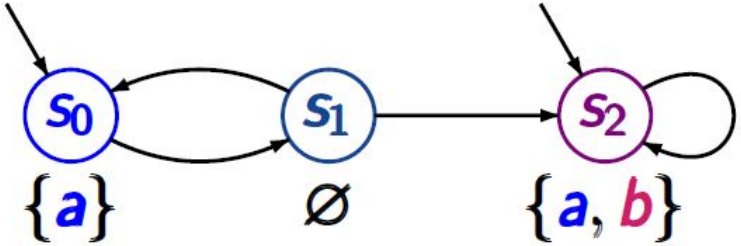
$\sigma \models \Diamond\varphi$ iff there exists $j \geq 0$ such that

$A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$

$\sigma \models \Box\varphi$ iff for all $j \geq 0$ we have:

$A_j\, A_{j+1}\, A_{j+2} \ldots \models \varphi$

Example: LTL-semantics over paths

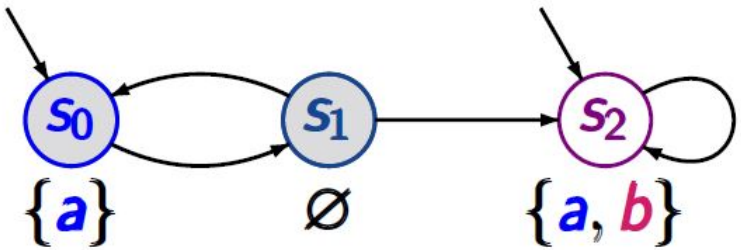


$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_2\, s_2\, s_2\, s_2 \ldots$ $\quad$ $trace(\pi) = \{a\}\, \varnothing\, \{a, b\}^\omega$

$\pi \models a$, but $\pi \not\models b$	as $L(s_0) = \{a\}$
$\pi \models \bigcirc(\neg a \wedge \neg b)$	as $L(s_1) = \varnothing$
$\pi \models \bigcirc\bigcirc(a \wedge b)$	as $L(s_2) = \{a, b\}$
$\pi \models (\neg b)\, \mathsf{U}\, (a \wedge b)$	as $s_0, s_1 \models \neg b$
$\pi \models (\neg b)\, \mathsf{U}\, \Box(a \wedge b)$	and $s_2 \models a \wedge b$

Correct or wrong?



$AP = \{a, b\}$

path $\pi = s_0\, s_1\, s_0\, s_1\, s_0\, s_1 \ldots$ $\qquad$ $trace(\pi) = (\{a\}\,\varnothing)^\omega$

$\pi \not\models a \,\mathsf{U}\, b$	as $s_0 \not\models b$ and $s_1 \not\models a \vee b$
$\pi \models \Diamond b \rightarrow (a \,\mathsf{U}\, b)$	as $\pi \not\models \Diamond b$
$\pi \models \bigcirc\bigcirc \neg b$	as $s_0 \models \neg b$
$\pi \not\models \Box a$	as $s_1 \not\models a$
$\pi \models \Box\Diamond a$	as $\Box\Diamond \mathrel{\widehat{=}}$ infinitely often
$\pi \not\models \Diamond\Box a$	as $\Diamond\Box \mathrel{\widehat{=}}$ eventually forever

LTL-semantics over TS

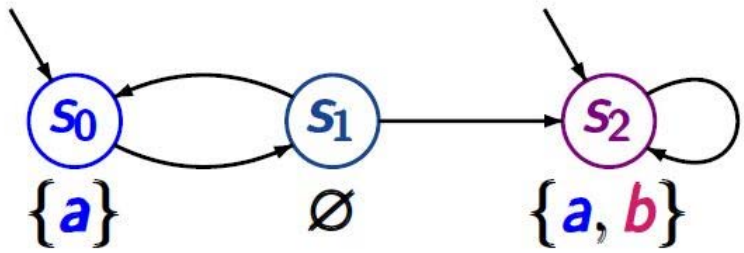
given a TS $\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$

define satisfaction relation $\models$ for

- **LTL** formulas over AP
- the maximal path fragments and states of $\mathcal{T}$

assumption: $\mathcal{T}$ has no terminal states, i.e.,
all maximal path fragments in $\mathcal{T}$ are infinite

Which formulas hold for TS?



$AP = \{a, b\}$

$\mathcal{T} \models a$ as $s_0 \models a$ and $s_2 \models a$

$\mathcal{T} \not\models \Diamond\Box a$ as $s_0\, s_1\, s_0\, s_1 \ldots \not\models \Diamond\Box a$

$\mathcal{T} \models \Diamond\Box b \vee \Box\Diamond(\neg a \wedge \neg b)$ as $s_2 \models b$, $s_1 \not\models a, b$

$\mathcal{T} \models \Box(a \rightarrow (\bigcirc\neg a \vee b))$ as $s_2 \models b$, $s_0 \models \bigcirc\neg a$

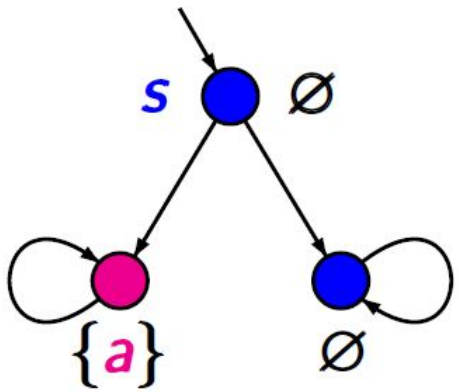
Correct or wrong?

For each path π we have: $\pi \models \varphi$ or $\pi \models \neg\varphi$

correct, since $\pi \models \neg\varphi$ iff $\pi \not\models \varphi$

For each state s we have: $s \models \varphi$ or $s \models \neg\varphi$

wrong.



$s \not\models \Diamond a$ and $s \not\models \neg\Diamond a$

LTL-formulas for MUTEX protocols

LTL formulas over $AP = \{\mathbf{wait}_1, \mathbf{crit}_1, \mathbf{wait}_2, \mathbf{crit}_2\}$

- the mutual exclusion property

$$\varphi_{mutex} = \Box(\neg \mathbf{crit}_1 \vee \neg \mathbf{crit}_2)$$

- "every process enters the critical section infinitely often"

$$\varphi_{live} = \Box\Diamond \mathbf{crit}_1 \wedge \Box\Diamond \mathbf{crit}_2$$

- starvation freedom

"every waiting process finally enters its critical section"

$$\varphi_{sf} = \Box(\mathbf{wait}_1 \rightarrow \Diamond \mathbf{crit}_1) \wedge \Box(\mathbf{wait}_2 \rightarrow \Diamond \mathbf{crit}_2)$$

Correct or wrong?

$$\Diamond(\varphi \vee \psi) \equiv \Diamond\varphi \vee \Diamond\psi$$

correct

$$\Diamond(\varphi \wedge \psi) \equiv \Diamond\varphi \wedge \Diamond\psi$$

wrong,
e.g.,

$$\models \Diamond b \wedge \Diamond a$$
$$\not\models \Diamond(b \wedge a)$$

---

similarly: $\Box(\varphi \wedge \psi) \equiv \Box\varphi \wedge \Box\psi$

$\Box(\varphi \vee \psi) \not\equiv \Box\varphi \vee \Box\psi$

Correct or wrong?

$\Diamond\Diamond\varphi \equiv \Diamond\varphi$

correct Analogous: $\Box\Box\varphi \equiv \Box\varphi$

$\bigcirc\Box\varphi \equiv \Box\bigcirc\varphi$

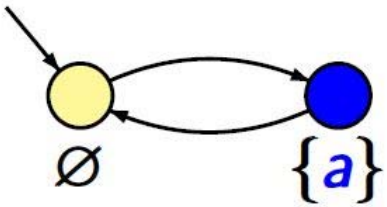
correct

$\Box\Diamond \mathrel{\widehat{=}}$ infinitely often

$\Diamond\Box \mathrel{\widehat{=}}$ eventually forever

$\Diamond\Box\varphi \equiv \Box\Diamond\varphi$

wrong



$\models \Box\Diamond a$

$\not\models \Diamond\Box a$

Linear Temporal Logic (LTL)

syntax and semantics of LTL

automata-based LTL model checking ⟵

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 ?

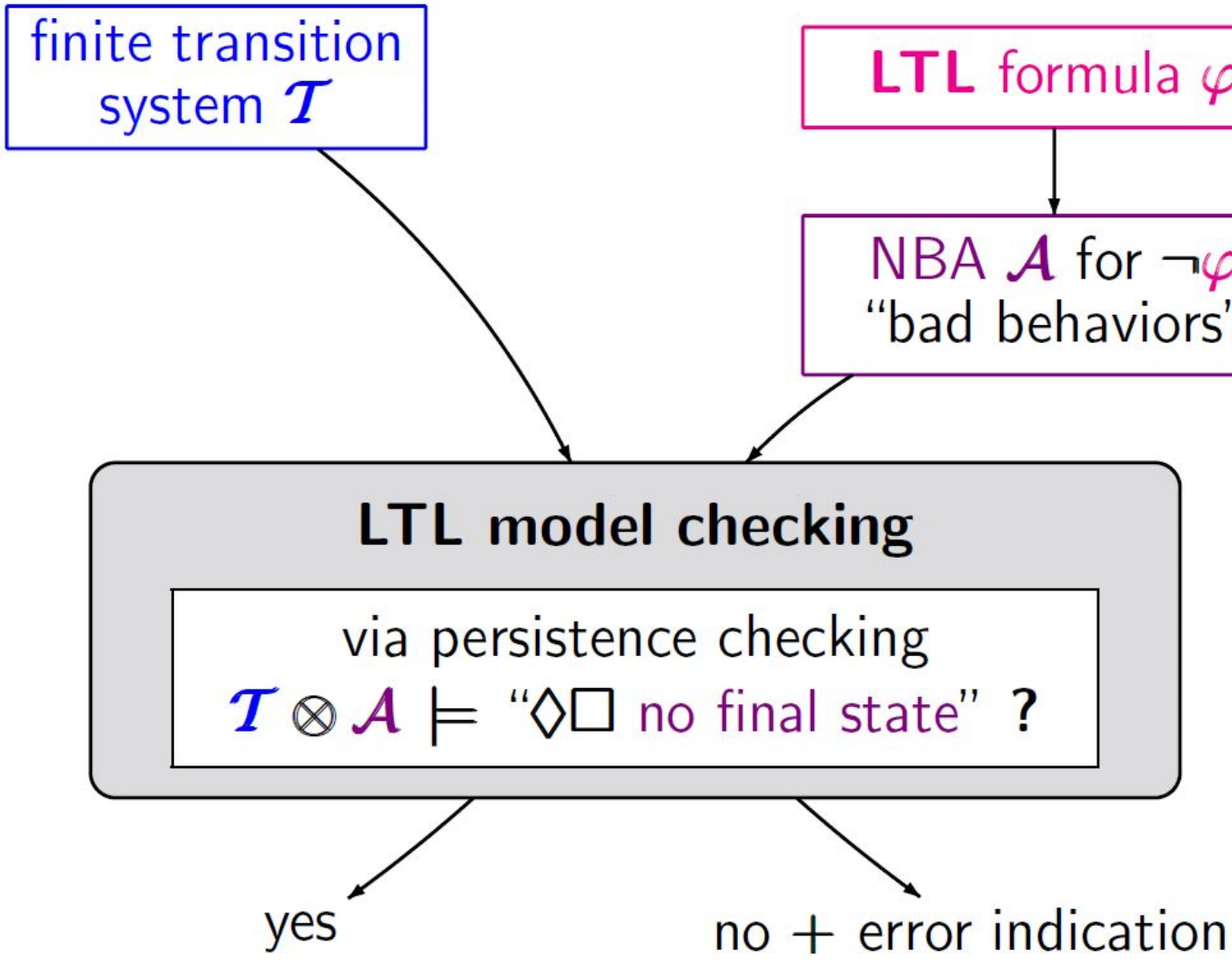
1. construct an **NBA** $\mathcal{A}$ for $Words(\neg\varphi)$
2. search a path π in $\mathcal{T}$ with

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

↑

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



Nondeterministic Buchii Automata (NBA)

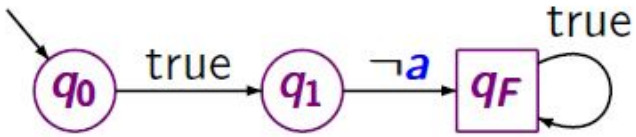
NBA $\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$

- 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

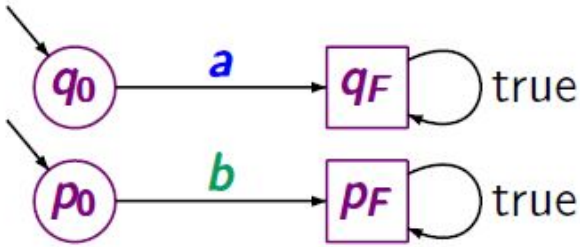
accepted language $\mathcal{L}_\omega(\mathcal{A}) \subseteq \Sigma^\omega$ is given by:

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

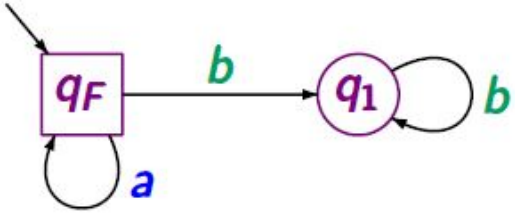
NBA for LTL formulas



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

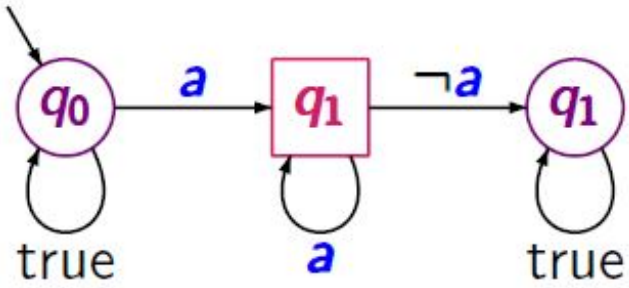


$$\mathcal{L}_\omega(\mathcal{A}) = \mathit{Words}(a \vee b)$$



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

NBA for LTL formulas

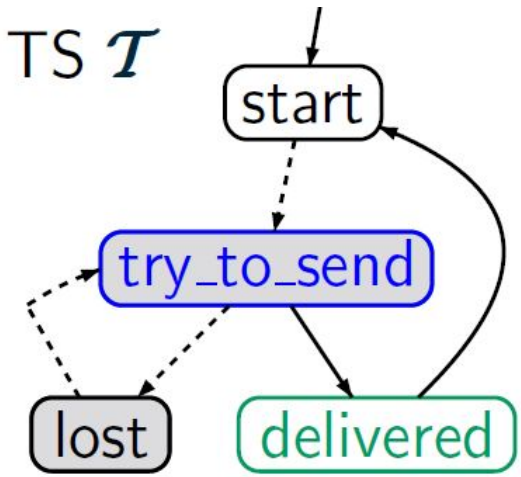


$$\mathcal{L}_\omega(\mathcal{A}) = \mathit{Words}(\Diamond\Box a)$$

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

$\vdots$

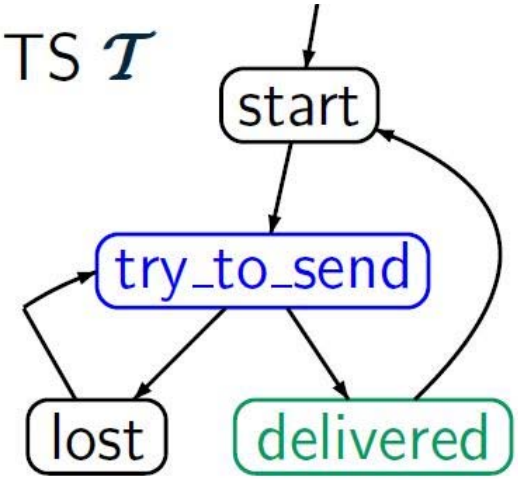


LTL formula $\varphi = \Box(\mathit{try} \rightarrow \Diamond \mathit{del})$

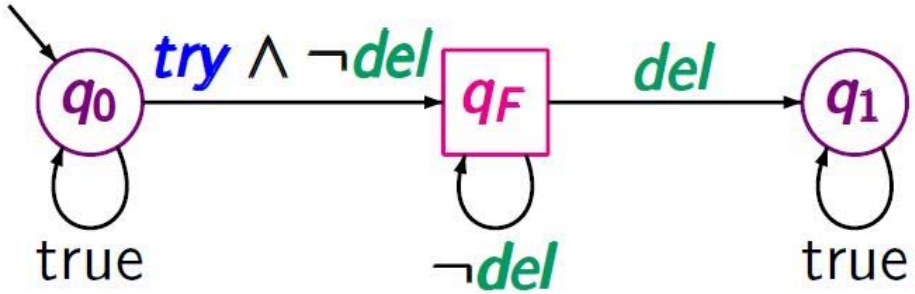
"each (repeatedly) sent message will eventually be delivered"

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

TS $\mathcal{T}$



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

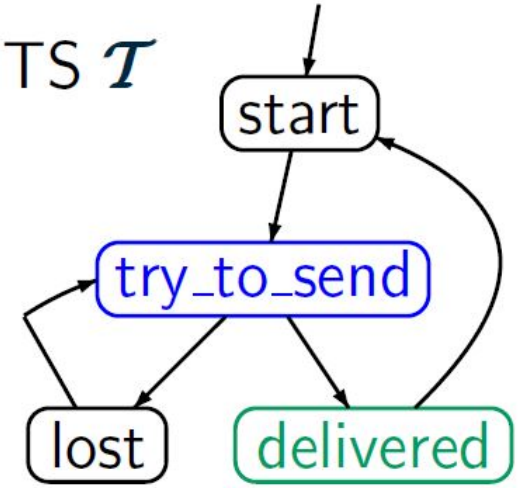


LTL formula $\varphi = \Box(\mathit{try} \rightarrow \Diamond\mathit{del})$

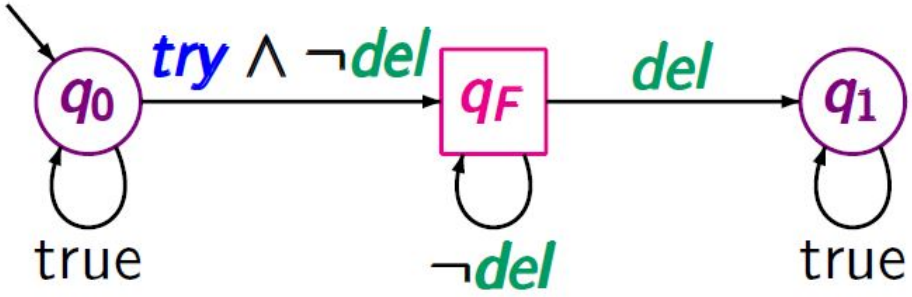
"each (repeatedly) sent message will eventually be delivered"

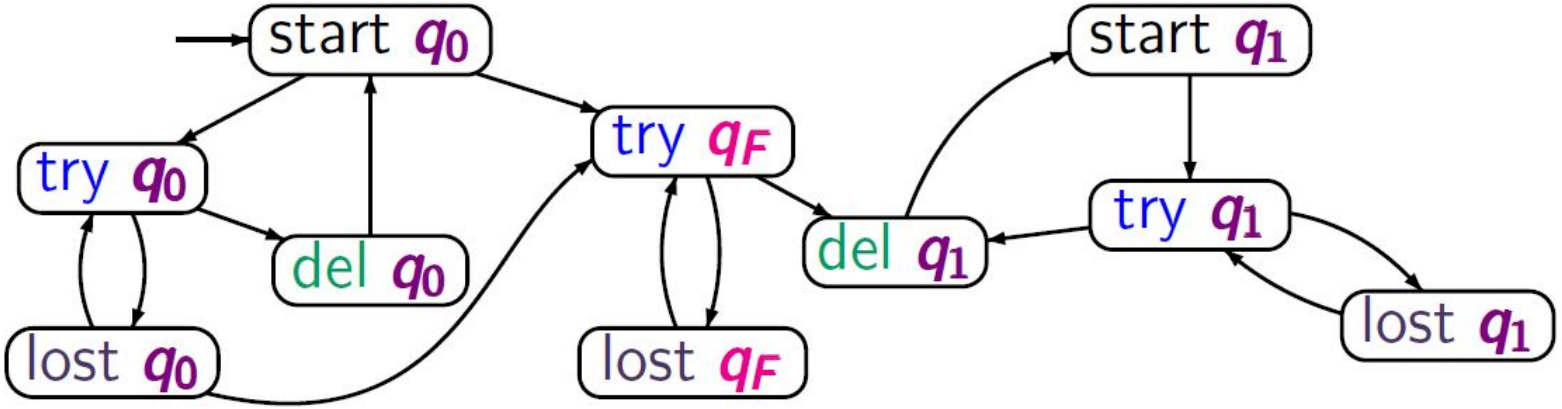
$\mathcal{T} \not\models \varphi$

TS $\mathcal{T}$



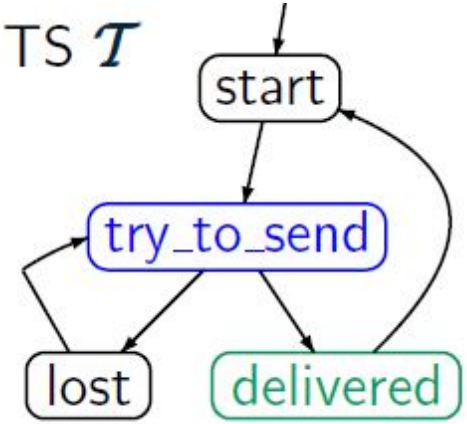
NBA $\mathcal{A}$ for $\neg\varphi \equiv \Diamond(\mathit{try} \wedge \Box\neg\mathit{del})$



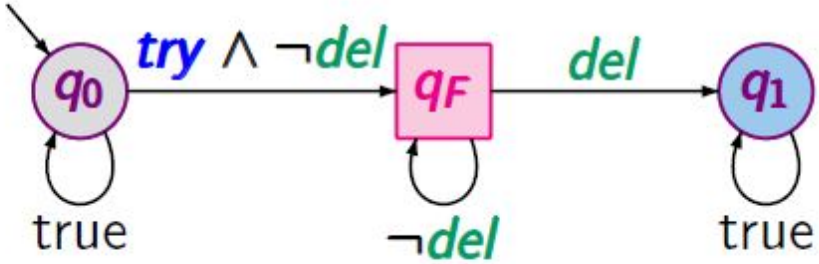


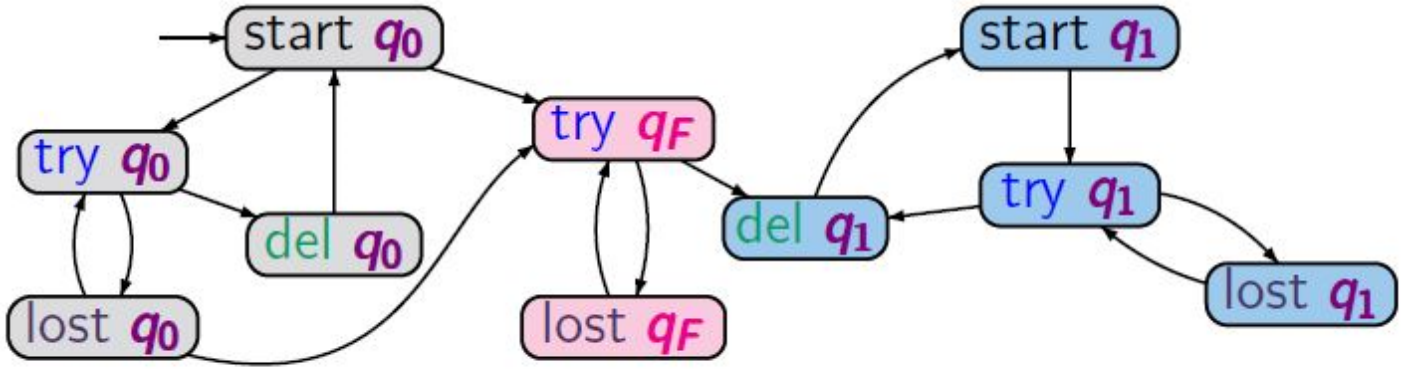
reachable fragment of the product-TS

TS $\mathcal{T}$

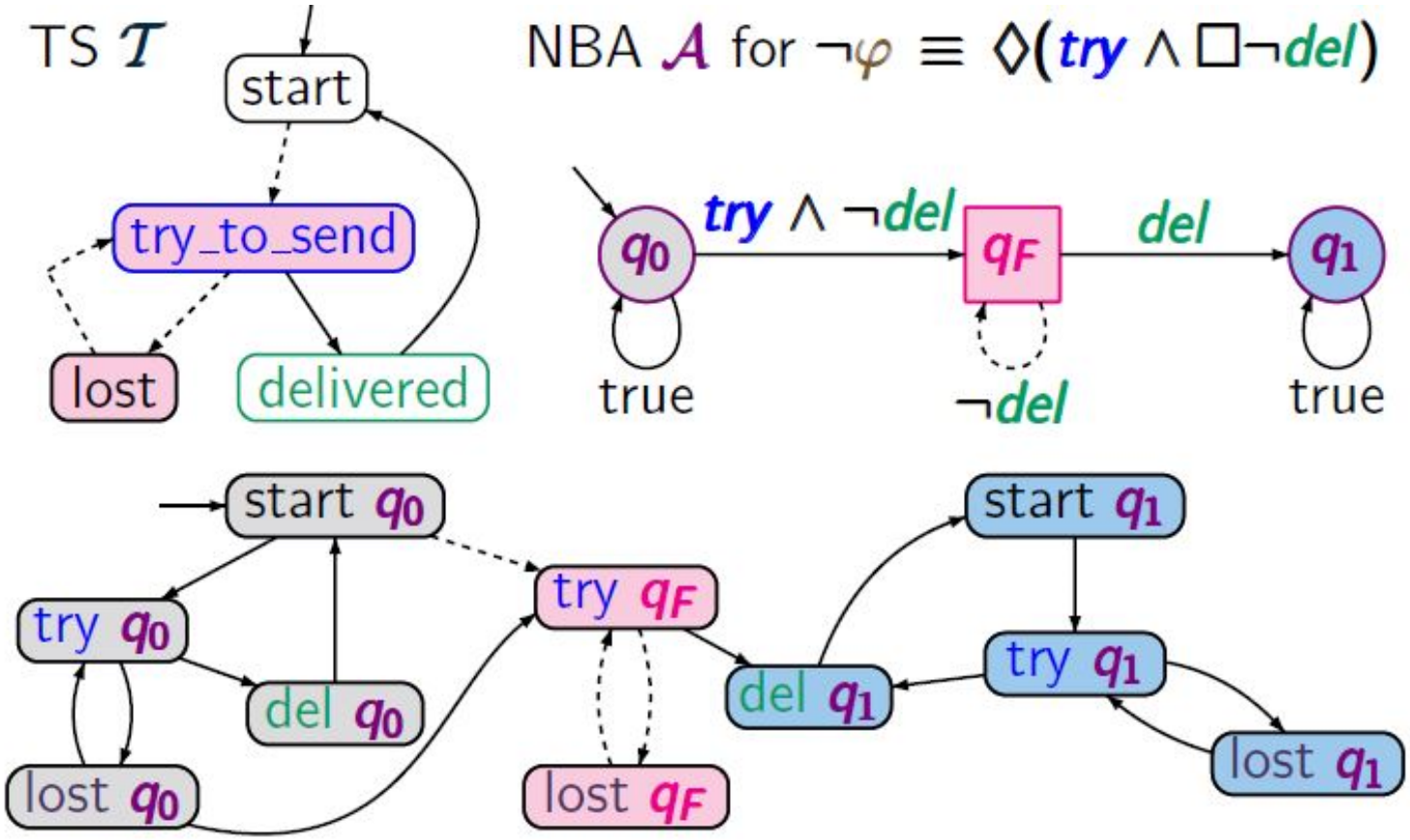


NBA $\mathcal{A}$ for $\neg\varphi \equiv \Diamond(try \wedge \Box\neg del)$





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


TS $\mathcal{T}$
start
try_to_send
lost
delivered
NBA $\mathcal{A}$ for $\neg\varphi \equiv \Diamond(try \wedge \Box\neg del)$
q_0
$try \wedge \neg del$
q_F
del
q_1
true
$\neg del$
true
start q_0
try q_0
del q_0
lost q_0
try q_F
lost q_F
del q_1
start q_1
try q_1
lost q_1