Introduction

Modelling parallel systems

Linear Time Properties

Regular Properties

- regular safety properties
- ω-regular properties
- model checking with Büchi automata $\longleftarrow$

Linear Temporal Logic

Computation-Tree Logic

Equivalences and Abstraction

Verifying ω-regular properties

given: finite transition system $\mathcal{T}$
ω-regular property E

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

Verifying ω-regular properties

given: finite transition system $\mathcal{T}$
ω-regular property E

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

(1) construct an **NBA** $\mathcal{A}$ for the bad behaviors, i.e.,
$\mathcal{L}_\omega(\mathcal{A}) = (2^{AP})^\omega \setminus E$

Verifying ω-regular properties

given: finite transition system $\mathcal{T}$

ω-regular property E

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

(1) construct an **NBA** $\mathcal{A}$ for the bad behaviors, i.e.,

$$\mathcal{L}_\omega(\mathcal{A}) = \left(2^{AP}\right)^\omega \setminus E$$

(2) check whether $Traces(\mathcal{T}) \cap \mathcal{L}_\omega(\mathcal{A}) = \varnothing$

given: finite transition system $\mathcal{T}$

ω-regular property E

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

(1) construct an **NBA** $\mathcal{A}$ for the bad behaviors, i.e.,
$\mathcal{L}_\omega(\mathcal{A}) \ = \ \big(2^{AP}\big)^\omega \setminus E$

(2) check whether $\mathit{Traces}(\mathcal{T}) \cap \mathcal{L}_\omega(\mathcal{A}) = \varnothing$

(3) build the product transition system $\mathcal{T} \otimes \mathcal{A}$ and check whether

$$\mathcal{T} \otimes \mathcal{A} \models \text{“never acceptance condition of } \mathcal{A}\text{”}$$

Verifying ω-regular properties

given: finite transition system $\mathcal{T}$
ω-regular property E

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

(1) construct an **NBA** $\mathcal{A}$ for the bad behaviors, i.e.,
$\mathcal{L}_\omega(\mathcal{A}) = (2^{AP})^\omega \setminus E$

(2) check whether $Traces(\mathcal{T}) \cap \mathcal{L}_\omega(\mathcal{A}) = \varnothing$

(3) build the product transition system $\mathcal{T} \otimes \mathcal{A}$ and check whether

$$\mathcal{T} \otimes \mathcal{A} \models \text{“never acceptance condition of } \mathcal{A}\text{”}$$

requires techniques for checking **persistence properties** in finite TS

Persistence property

Persistence property

Let E be an LT-property, i.e., $E \subseteq \left(2^{AP}\right)^{\omega}$

E is called a persistence property if there exists a propositional formula Φ over AP such that

$$E = \left\{ \begin{array}{c} \text{set of all infinite words } A_0\, A_1\, A_2 \ldots \in \left(2^{AP}\right)^{\omega} \\ \text{s.t.} \quad \overset{\infty}{\forall}\, i \geq 0.\ A_i \models \Phi \end{array} \right.$$

$\overset{\infty}{\forall}\, i{\geq}0. \ldots = \exists j{\geq}0\ \forall i{\geq}j. \ldots$ "for all but finitely many"

Persistence property

Let E be an LT-property, i.e., $E \subseteq (2^{AP})^\omega$

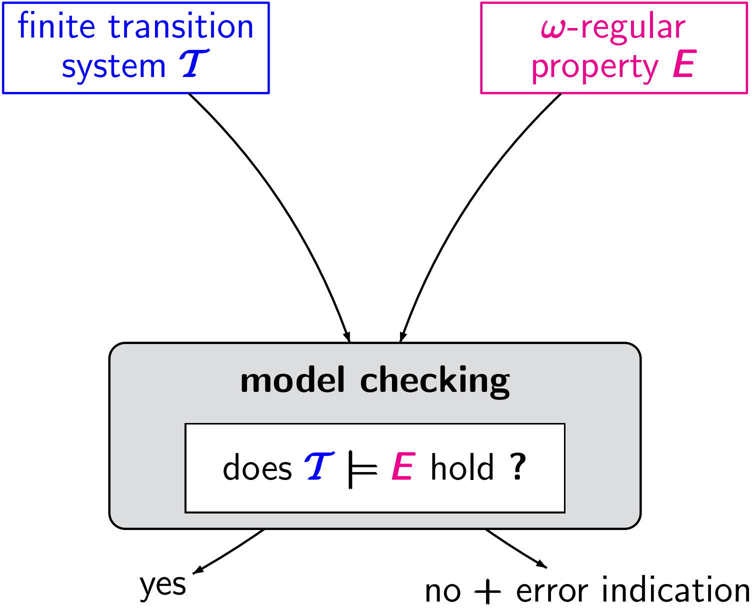
E is called a persistence property if there exists a propositional formula Φ over AP such that

$$E = \left\{ \begin{array}{l} \text{set of all infinite words } A_0\, A_1\, A_2 \ldots \in (2^{AP})^\omega \\ \qquad\qquad \text{s.t.} \quad \overset{\infty}{\forall}\, i \geq 0.\ A_i \models \Phi \end{array} \right.$$

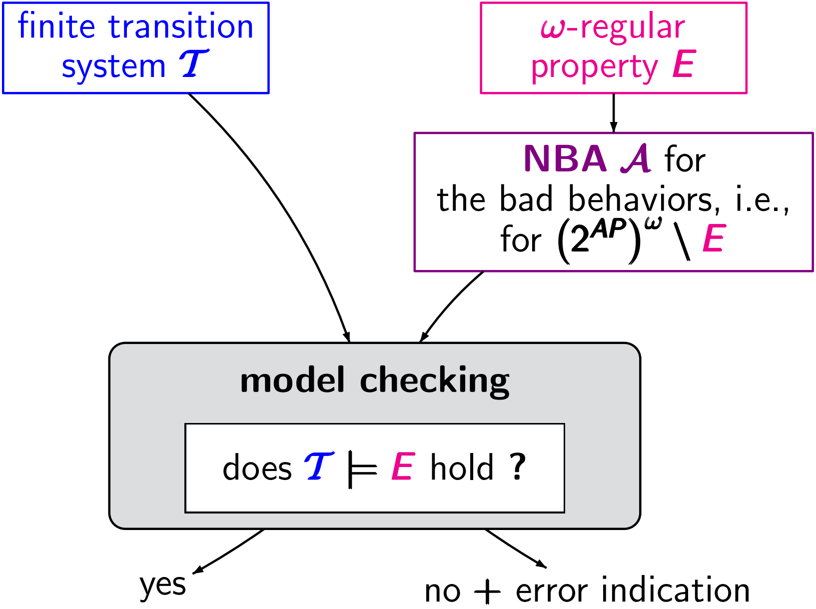
"from some moment on Φ"
"eventually forever Φ"

$\overset{\infty}{\forall}\, i{\geq}0. \ldots = \exists j{\geq}0\ \forall i{\geq}j. \ldots$ "for all but finitely many"

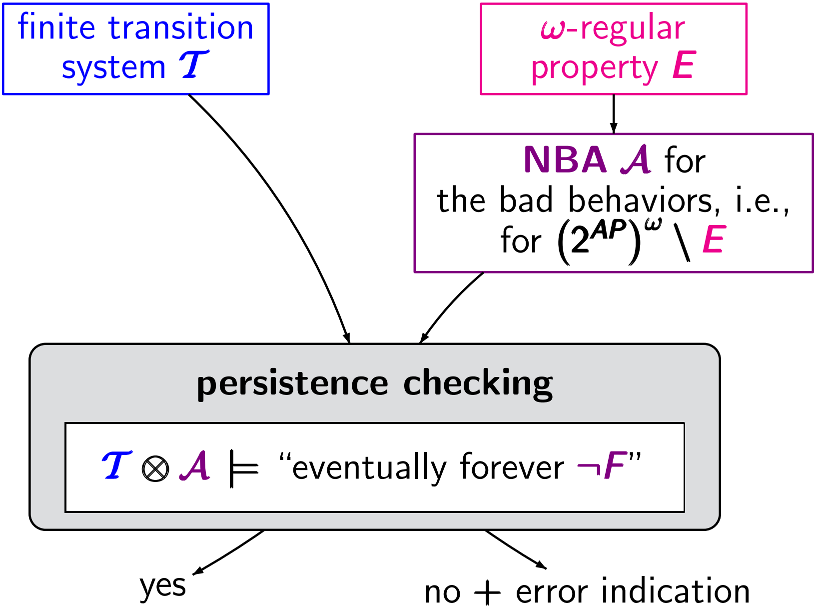
Checking ω-regular properties



Checking ω-regular properties



Checking ω-regular properties



Recall: product of a TS and an NFA

finite transition system
$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$

NFA for bad prefixes
$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$

path
fragment $\widehat{\pi}$

Recall: product of a TS and an NFA

finite transition system
$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$

NFA for bad prefixes
$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$

s_0	$L(s_0) = A_0$
$\downarrow$	
s_1	$L(s_1) = A_1$
$\downarrow$	
s_2	$L(s_2) = A_2$
$\downarrow$	
$\vdots$	$\vdots$
$\downarrow$	
s_n	$L(s_n) = A_n$
path fragment $\widehat{\pi}$	trace

Recall: product of a TS and an NFA

finite transition system
$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$

NFA for bad prefixes
$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$

$s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots \rightarrow s_n$

$L(s_0) = A_0$
$L(s_1) = A_1$
$L(s_2) = A_2$
$\vdots$
$L(s_n) = A_n$

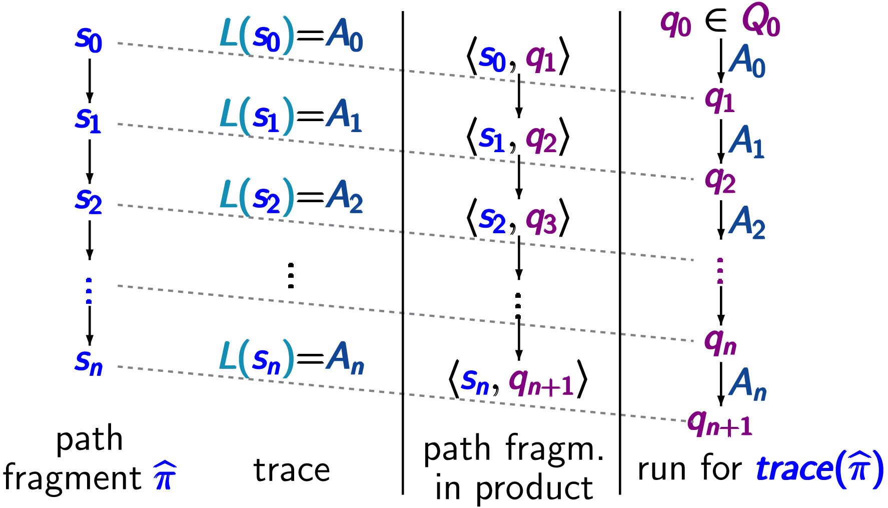
$q_0 \in Q_0 \xrightarrow{A_0} q_1 \xrightarrow{A_1} q_2 \xrightarrow{A_2} \ldots \rightarrow q_n \xrightarrow{A_n} q_{n+1}$

path fragment $\widehat{\pi}$ | trace | run for $trace(\widehat{\pi})$

Recall: product of a TS and an NFA

finite transition system
$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$

NFA for bad prefixes
$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$



Product transition system

recall: definition of the product of a **TS** and **NFA**

Product transition system

$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$ transition system

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

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

Product transition system

$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$ transition system

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

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

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

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

Product transition system

$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$ transition system

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

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

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

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

set of atomic propositions: $AP' = Q$

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

Product transition system

$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$ transition system

$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$ NFA $\longleftarrow$ same definition for **NBA**

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

$$\frac{s \stackrel{\alpha}{\longrightarrow} s' \quad \wedge \quad q' \in \delta(q, L(s'))}{\langle s, q \rangle \stackrel{\alpha}{\longrightarrow}' \langle s', q' \rangle}$$

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

set of atomic propositions: $AP' = Q$

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

Product of a TS and NBA

$\mathcal{T} = (S, Act, \rightarrow, S_0, AP, L)$ transition system

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

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

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

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

set of atomic propositions: $AP' = Q$

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

ω-regular model checking

given:	finite TS $\mathcal{T}$
	ω-regular LT property E
question:	does $\mathcal{T} \models E$ hold **?**

ω-regular model checking

given:	finite TS $\mathcal{T}$
	ω-regular LT property E
question:	does $\mathcal{T} \models E$ hold **?**

algorithm uses an **NBA** for the bad behaviors for E

ω-regular model checking

given:	finite TS $\mathcal{T}$
	ω-regular LT property E
question:	does $\mathcal{T} \models E$ hold ?

algorithm uses an **NBA** for the bad behaviors for E

relies on a reduction to the persistence checking problem

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

$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$ non-blocking NBA

representing the bad behaviors of an ω-regular LT-property E

ω-regular model checking

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

$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$ non-blocking NBA

representing the bad behaviors of an ω-regular LT-property E, i.e., $\mathcal{L}_\omega(\mathcal{A}) = (2^{AP})^\omega \setminus E$

ω-regular model checking

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

$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$ non-blocking NBA

representing the bad behaviors of an ω-regular LT-property E, i.e., $\mathcal{L}_\omega(\mathcal{A}) = \left(2^{AP}\right)^\omega \setminus E$

The following statements are equivalent:

(1) $\mathcal{T} \models E$

(2) $Traces(\mathcal{T}) \cap \mathcal{L}_\omega(\mathcal{A}) = \varnothing$

$\mathcal{T} = (S, Act, \longrightarrow, S_0, AP, L)$ finite transition system without terminal states

$\mathcal{A} = (Q, 2^{AP}, \delta, Q_0, F)$ non-blocking NBA

representing the bad behaviors of an ω-regular LT-property E, i.e., $\mathcal{L}_\omega(\mathcal{A}) = \left(2^{AP}\right)^\omega \setminus E$

The following statements are equivalent:

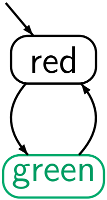
(1) $\mathcal{T} \models E$

(2) $Traces(\mathcal{T}) \cap \mathcal{L}_\omega(\mathcal{A}) = \varnothing$

(3) $\mathcal{T} \otimes \mathcal{A} \models$ "eventually forever $\neg F$"

Example: ω-regular model checking

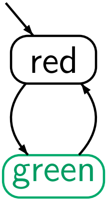
TS $\mathcal{T}$



LT property: "infinitely often green"

Example: ω-regular model checking

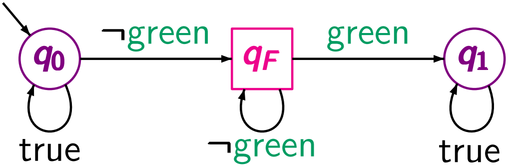
TS $\mathcal{T}$



LT property: "infinitely often green"

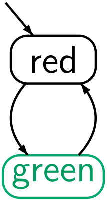
NBA $\mathcal{A}$ for the complement

"from some moment on ¬green"



Example: ω-regular model checking

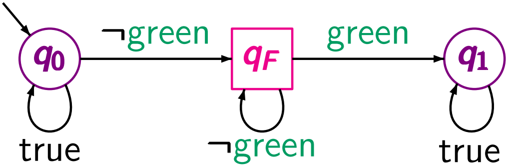
TS $\mathcal{T}$

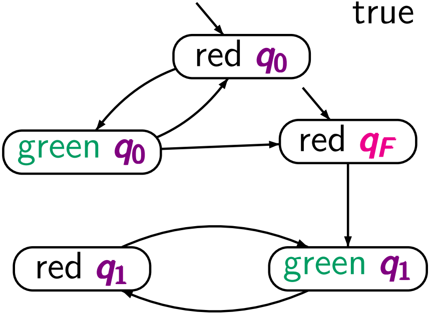


LT property: "infinitely often green"

NBA $\mathcal{A}$ for the complement

"from some moment on $\neg$green"

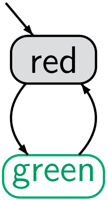




reachable fragment of the product TS $\mathcal{T} \otimes \mathcal{A}$

Example: ω-regular model checking

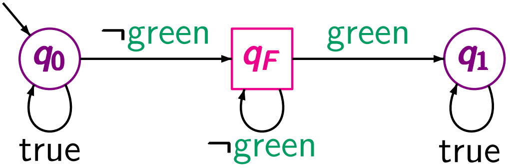
TS $\mathcal{T}$

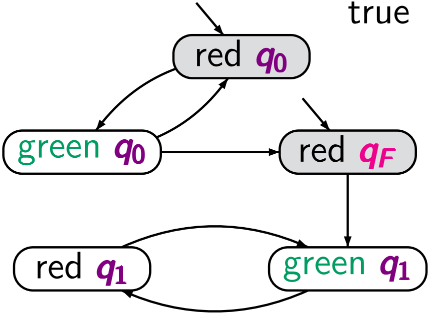


LT property: "infinitely often green"

NBA $\mathcal{A}$ for the complement

"from some moment on $\neg$green"





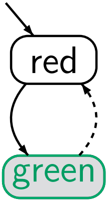
initial states:

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

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

Example: ω-regular model checking

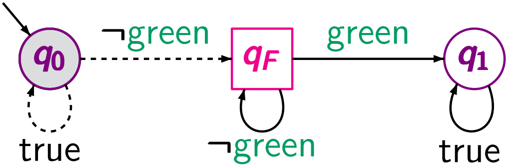
TS $\mathcal{T}$

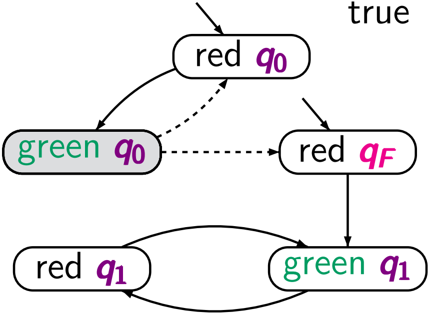


LT property: "infinitely often green"

NBA $\mathcal{A}$ for the complement

"from some moment on ¬green"





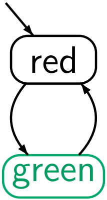
transition

$\langle \text{green}, q_0 \rangle \longrightarrow \langle \text{red}, q \rangle$

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

Example: ω-regular model checking

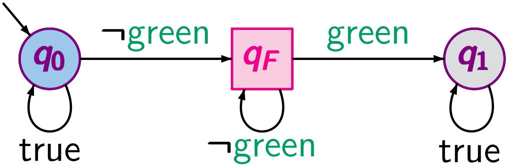
TS $\mathcal{T}$

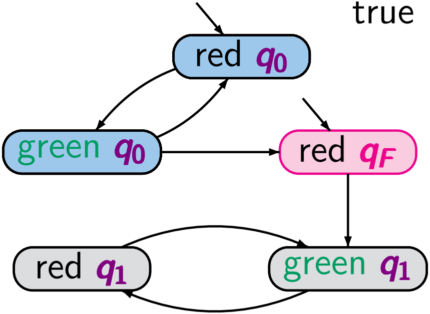


LT property: "infinitely often green"

NBA $\mathcal{A}$ for the complement

"from some moment on $\neg$green"





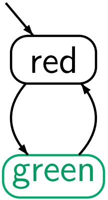
atomic propositions

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

obvious labeling function

Example: ω-regular model checking

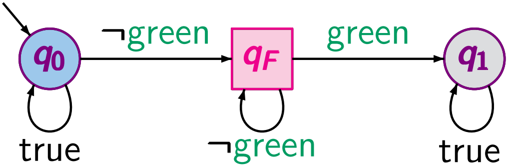
TS $\mathcal{T}$

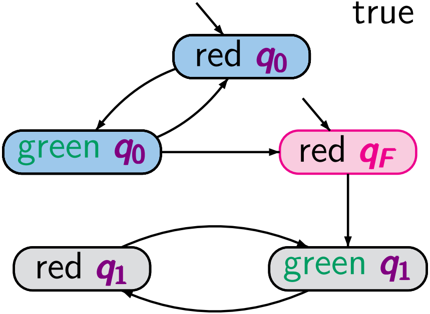


LT property: "infinitely often green"

NBA $\mathcal{A}$ for the complement

"from some moment on $\neg$green"





atomic propositions

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

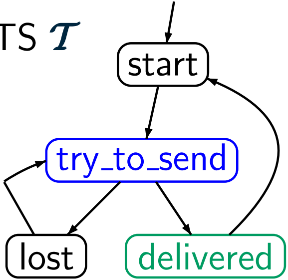
obvious labeling function

$\mathcal{T} \otimes \mathcal{A} \models$

"eventually forever $\neg F$"

Example: ω-regular model checking

TS $\mathcal{T}$

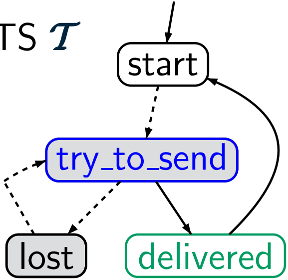


ω-regular LT property E:

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

Example: ω-regular model checking

TS $\mathcal{T}$



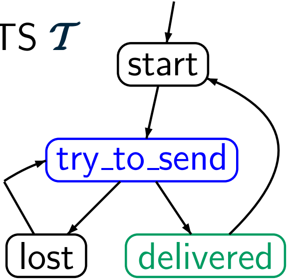
ω-regular LT property E:

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

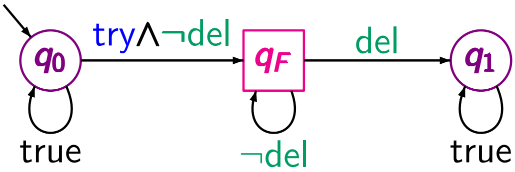
$\mathcal{T} \not\models E$

Example: ω-regular model checking

TS $\mathcal{T}$



NBA $\mathcal{A}$ for the bad behaviors



ω-regular LT property E:

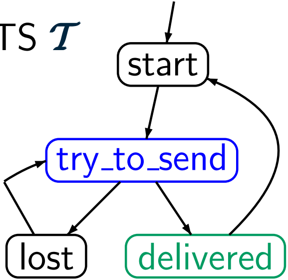
"each (repeatedly) sent message will eventually be delivered"

complement of E, i.e., LT property for the bad behaviors:

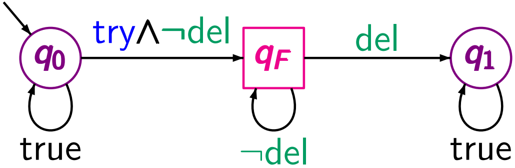
"never delivered after some trial"

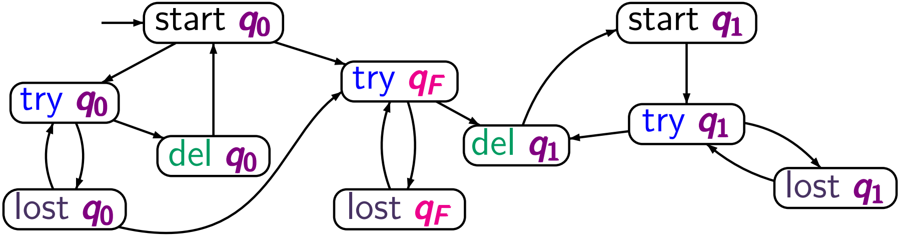
Example: ω-regular model checking

TS $\mathcal{T}$



NBA $\mathcal{A}$ for the bad behaviors

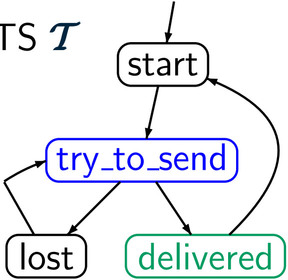




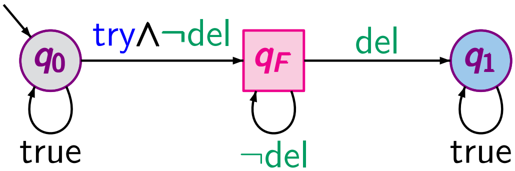
reachable fragment of the product-TS

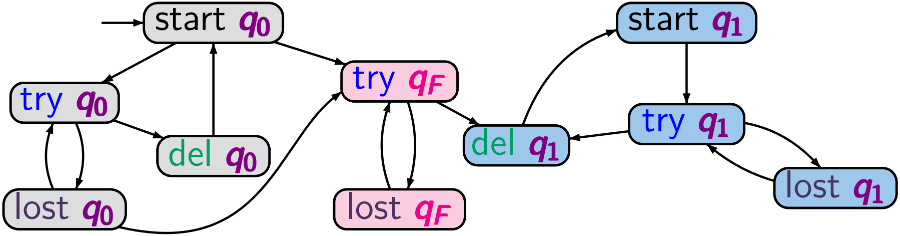
Example: ω-regular model checking

TS $\mathcal{T}$



NBA $\mathcal{A}$ for the bad behaviors

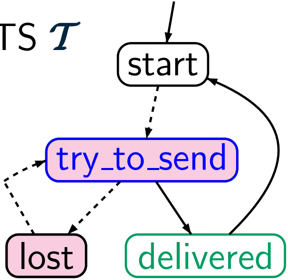




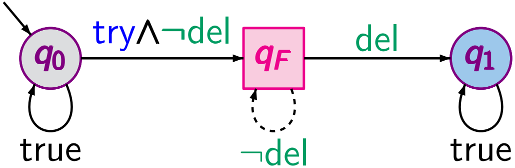
set of atomic propositions $AP' = \{q_0, q_1, q_F\}$

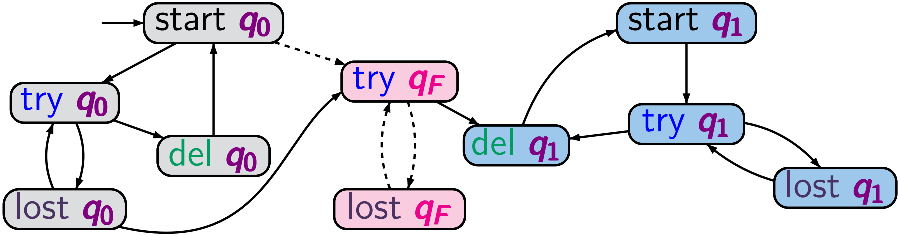
Example: ω-regular model checking

TS $\mathcal{T}$



NBA $\mathcal{A}$ for the bad behaviors





$\mathcal{T} \otimes \mathcal{A} \not\models$ "eventually forever $\neg F$"

Checking safety and ω-regular properties

Checking safety and ω-regular properties

for regular safety property E

$$\mathcal{T} \models E$$

iff $Traces_{fin}(\mathcal{T}) \cap BadPref = \varnothing$

Checking safety and ω-regular properties

for regular safety property E

$$\mathcal{T} \models E$$

iff $\mathit{Traces}_{\mathit{fin}}(\mathcal{T}) \cap \mathit{BadPref} = \varnothing$

for ω-regular property E

$$\mathcal{T} \models E$$

iff $\mathit{Traces}(\mathcal{T}) \cap \mathcal{L}_\omega(\mathcal{A}) = \varnothing$

$\mathcal{A}$ is an **NBA** for the bad behaviors of E

Checking safety and ω-regular properties

for regular safety property E

$$\mathcal{T} \models E$$

iff $\quad Traces_{fin}(\mathcal{T}) \cap \mathcal{L}(\mathcal{A}) = \varnothing$

$\mathcal{A}$ is an **NFA** for the bad prefixes of E

for ω-regular property E

$$\mathcal{T} \models E$$

iff $\quad Traces(\mathcal{T}) \cap \mathcal{L}_\omega(\mathcal{A}) = \varnothing$

$\mathcal{A}$ is an **NBA** for the bad behaviors of E

Checking safety and ω-regular properties

for regular safety property E

$$\mathcal{T} \models E$$

iff $\quad Traces_{fin}(\mathcal{T}) \cap \mathcal{L}(\mathcal{A}) = \varnothing$

iff $\quad \mathcal{T} \otimes \mathcal{A} \models$ "forever $\neg F$"

$\mathcal{A}$ is an **NFA** for the bad prefixes of E

for ω-regular property E

$$\mathcal{T} \models E$$

iff $\quad Traces(\mathcal{T}) \cap \mathcal{L}_\omega(\mathcal{A}) = \varnothing$

iff $\quad \mathcal{T} \otimes \mathcal{A} \models$ "eventually forever $\neg F$"

$\mathcal{A}$ is an **NBA** for the bad behaviors of E

F = set of final states in $\mathcal{A}$

Checking safety and ω-regular properties

for regular safety property E

$$\mathcal{T} \models E$$

iff $Traces_{fin}(\mathcal{T}) \cap \mathcal{L}(\mathcal{A}) = \varnothing$

iff $\mathcal{T} \otimes \mathcal{A} \models$ "forever $\neg F$" ← **invariant checking**

for ω-regular property E

$$\mathcal{T} \models E$$

iff $Traces(\mathcal{T}) \cap \mathcal{L}_\omega(\mathcal{A}) = \varnothing$

iff $\mathcal{T} \otimes \mathcal{A} \models$ "eventually forever $\neg F$" ← **persistence checking**

F = set of final states in $\mathcal{A}$

Persistence checking

given:	finite transition system $\mathcal{T}$ over AP
	persistence condition $a \in AP$
question:	does $\mathcal{T} \models$ "eventually forever a" hold **?**

Persistence checking

given:	finite transition system $\mathcal{T}$ over AP persistence condition $a \in AP$
question:	does $\mathcal{T} \models$ "eventually forever a" hold **?**

$\mathcal{T} \not\models$ "eventually forever a"

iff there is a path $s_0\, s_1\, s_2\, s_3 \ldots$ in $\mathcal{T}$ s.t.
$s_i \not\models a$ for infinitely many $i \geq 0$

Persistence checking

given:	finite transition system $\mathcal{T}$ over AP
	persistence condition $a \in AP$
question:	does $\mathcal{T} \models$ "eventually forever a" hold ?

$\mathcal{T} \not\models$ "eventually forever a"

iff there is a path $s_0\, s_1\, s_2\, s_3 \ldots$ in $\mathcal{T}$ s.t.
$s_i \not\models a$ for infinitely many $i \geq 0$

iff there exists a reachable state s with $s \not\models a$
and a cycle $s \ldots s$

given:	finite transition system $\mathcal{T}$ over AP persistence condition $a \in AP$
question:	does $\mathcal{T} \models$ "eventually forever a" hold ?

$\mathcal{T} \not\models$ "eventually forever a"

iff there is a path $s_0\, s_1\, s_2\, s_3 \ldots$ in $\mathcal{T}$ s.t.
$s_i \not\models a$ for infinitely many $i \geq 0$

iff there exists a reachable state s with $s \not\models a$
and a cycle $s \ldots s$

iff there exists a non-trivial reachable SCC C
with $C \cap \{s \in S : s \not\models a\} \neq \varnothing$

given:	finite transition system $\mathcal{T}$ over AP
	persistence condition $a \in AP$
question:	does $\mathcal{T} \models$ "eventually forever a" hold **?**

$\mathcal{T} \not\models$ "eventually forever a"

iff there exists a reachable state s with $s \not\models a$ and a cycle $s \ldots s$

iff there exists a non-trivial reachable **SCC** C with $C \cap \{s \in S : s \not\models a\} \neq \varnothing$ ↑

SCC: strongly connected component, i.e., maximal set of states that are reachable from each other

given:	finite transition system $\mathcal{T}$ over AP persistence condition $a \in AP$
question:	does $\mathcal{T} \models$ "eventually forever a" hold ?

$\mathcal{T} \not\models$ "eventually forever a"

iff there exists a reachable state s with $s \not\models a$ and a cycle $s \dots s$

iff there exists a non-trivial reachable **SCC** C with $C \cap \{s \in S : s \not\models a\} \neq \varnothing$

A SCC is called non-trivial if it has at least one edge.
"either 1 state with a self-loop or 2 or more states"

Persistence checking

given:	finite transition system $\mathcal{T}$ over AP
	persistence condition $a \in AP$
question:	does $\mathcal{T} \models$ "eventually forever a" hold **?**

$\mathcal{T} \not\models$ "eventually forever a"

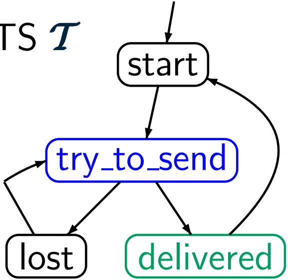
iff there exists a reachable state s with $s \not\models a$ and a cycle $s \ldots s$

iff there exists a non-trivial reachable **SCC** C with $C \cap \{s \in S : s \not\models a\} \neq \varnothing$

method: calculate and analyze the **SCCs**

Example: ω-regular model checking

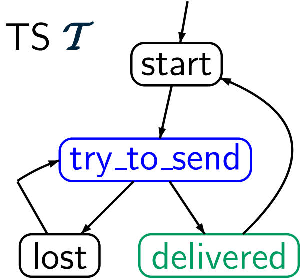
TS $\mathcal{T}$

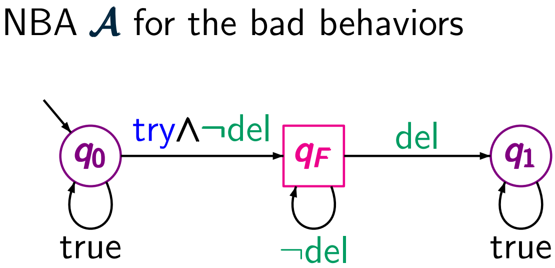


ω-regular LT property E:

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

Example: ω-regular model checking



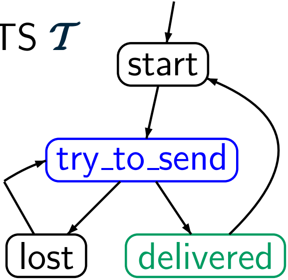


ω-regular LT property E:

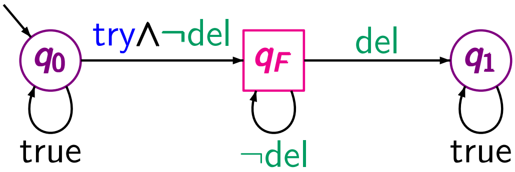
"each (repeatedly) sent message will eventually be delivered"

Example: ω-regular model checking

TS $\mathcal{T}$



NBA $\mathcal{A}$ for the bad behaviors

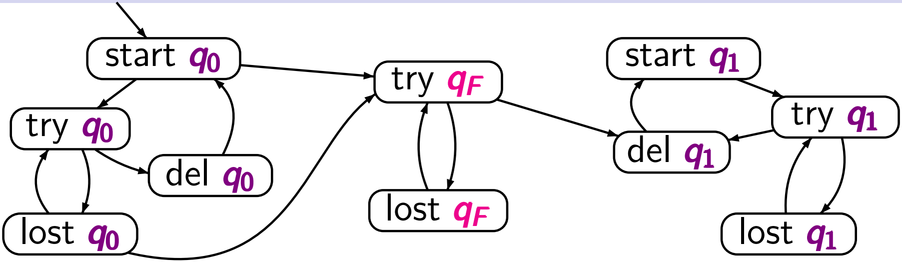


ω-regular LT property E:

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

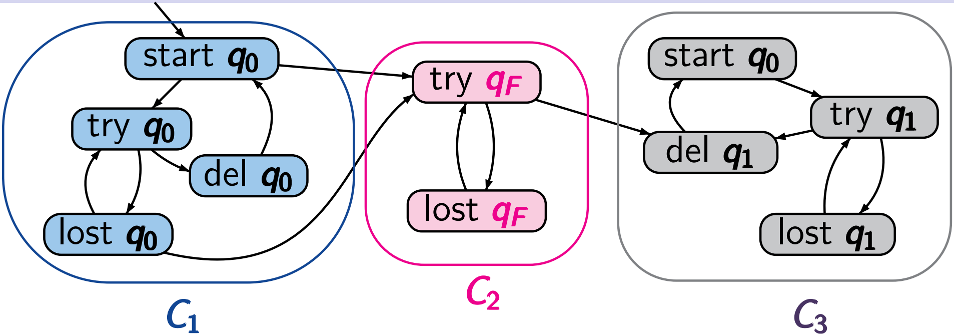
... analysis of the **SCCs** in product $\mathcal{T} \otimes \mathcal{A}$...

Example: persistence checking $\mathcal{T} \otimes \mathcal{A}$



persistence property: "eventually forever $\neg q_F$"

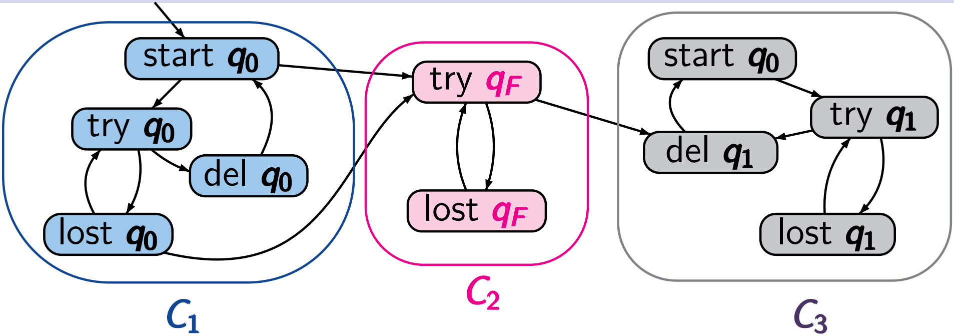
Example: persistence checking $\mathcal{T} \otimes \mathcal{A}$



persistence property: "eventually forever $\neg q_F$"

3 reachable SCCs: C_1, C_2, C_3

Example: persistence checking $\mathcal{T} \otimes \mathcal{A}$

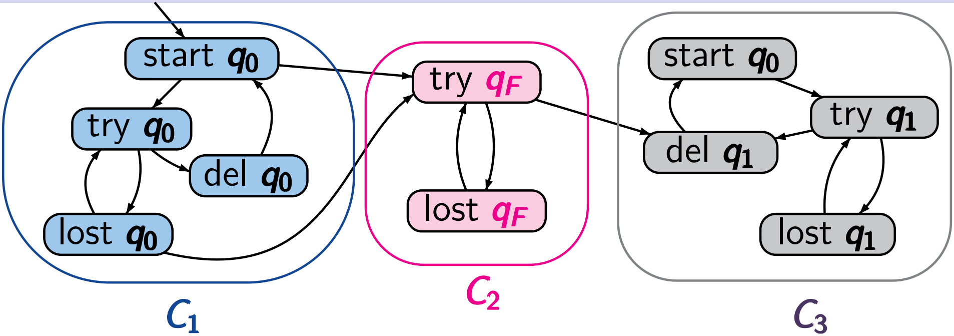


persistence property: "eventually forever $\neg q_F$"

3 reachable SCCs: C_1, C_2, C_3

C_2 non-trivial, and contains two states s with $s \not\models \neg q_F$

Example: persistence checking $\mathcal{T} \otimes \mathcal{A}$



persistence property: "eventually forever $\neg q_F$"

3 reachable SCCs: C_1, C_2, C_3

C_2 non-trivial, and contains two states s with $s \not\models \neg q_F$

$$\mathcal{T} \otimes \mathcal{A} \not\models \text{"eventually forever } \neg q_F\text{"}$$

Persistence checking algorithms based on ...

$\mathcal{T} \not\models$ "eventually forever a"

iff there exists a reachable state s with $s \not\models a$ and a cycle $s \ldots s$

iff there exists a non-trivial reachable **SCC** C with $C \cap \{s \in S : s \not\models a\} \neq \varnothing$