Overview

Introduction

Modelling parallel systems

Linear Time Properties

Regular Properties

Linear Temporal Logic (LTL)

Computation-Tree Logic

Equivalences and Abstraction

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

Examples for LTL formulas

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

eventually

$$\Diamond\varphi \stackrel{\text{def}}{=} \mathit{true}\,\mathsf{U}\,\varphi$$

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

Semantics of LTL over infinite words

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

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

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

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

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

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

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

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

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

Overview

Introduction

Modelling parallel systems

Linear Time Properties

Regular Properties

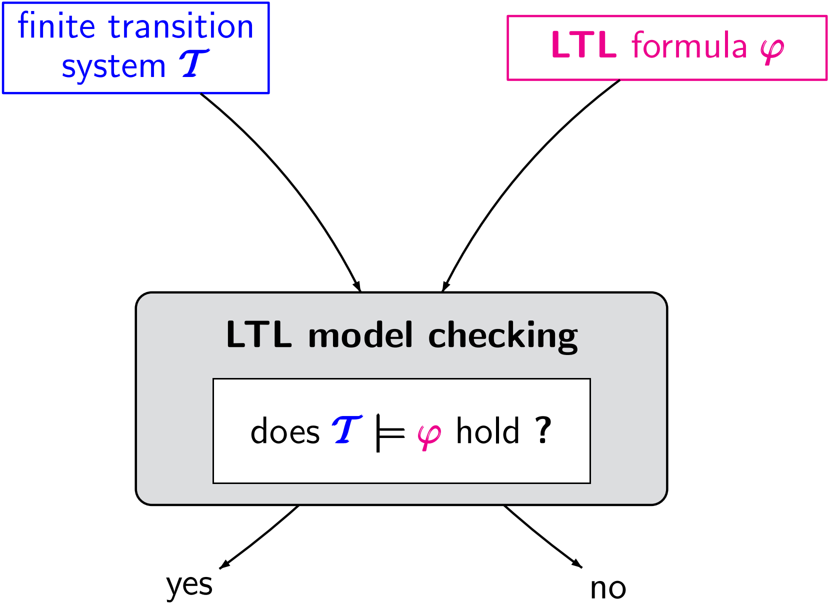
Linear Temporal Logic (LTL)

- syntax and semantics of LTL
- automata-based LTL model checking ⟵
- complexity of LTL model checking

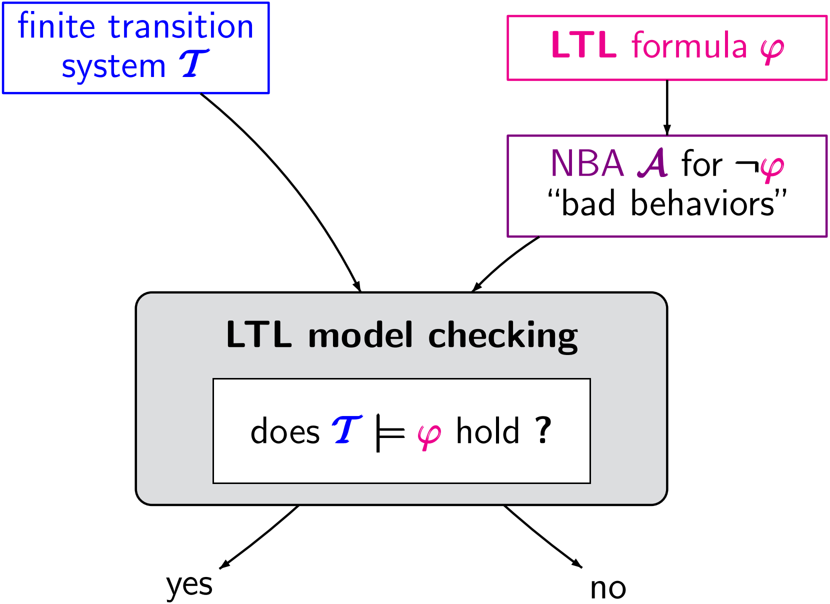
Computation-Tree Logic

Equivalences and Abstraction

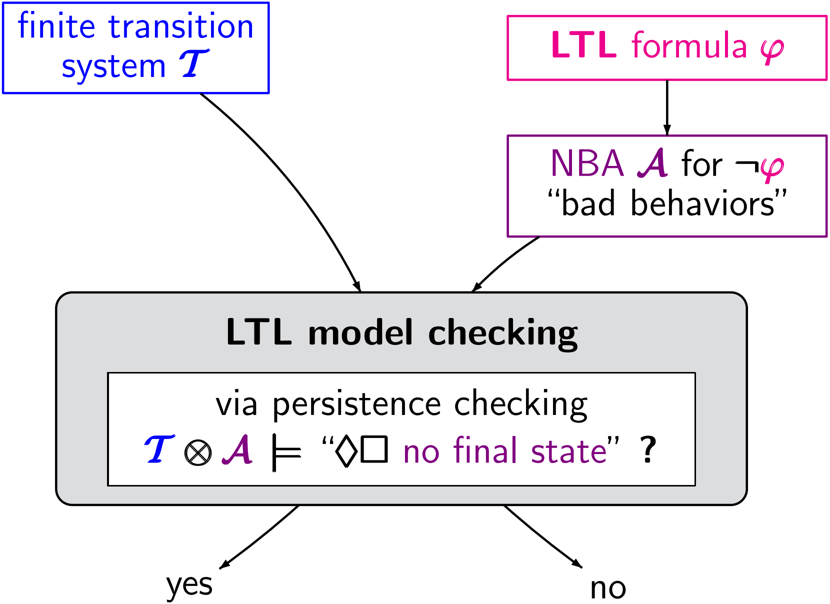
Automata-based LTL model checking



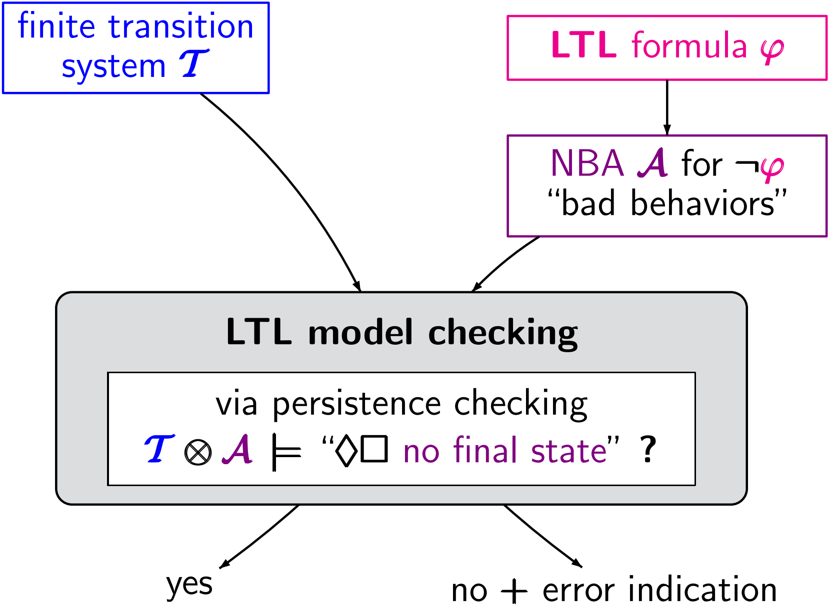
Automata-based LTL model checking



Automata-based LTL model checking



Automata-based LTL model checking



From LTL to NBA

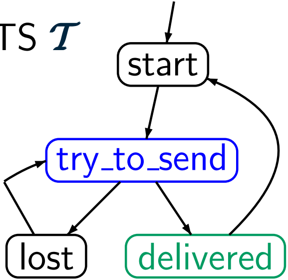
For each **LTL** formula φ over AP there is an **NBA** $\mathcal{A}$ over the alphabet 2^{AP} such that

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

proof: ... later ...

Example: LTL model checking

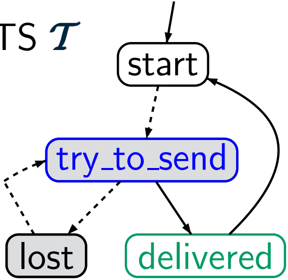
TS $\mathcal{T}$



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

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

TS $\mathcal{T}$



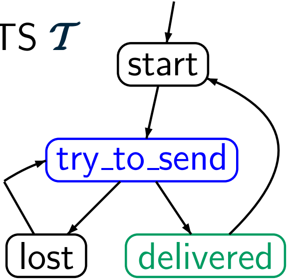
LTL formula $\varphi = \Box(\boldsymbol{try} \rightarrow \Diamond \boldsymbol{del})$

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

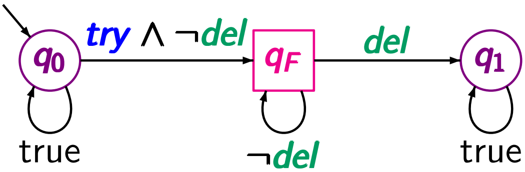
$\mathcal{T} \not\models \varphi$

Example: LTL model checking

TS $\mathcal{T}$



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



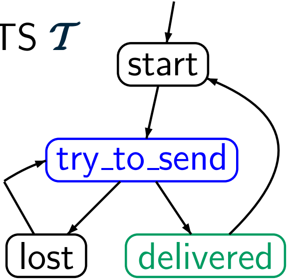
LTL formula $\varphi = \Box(try \rightarrow \Diamond del)$

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

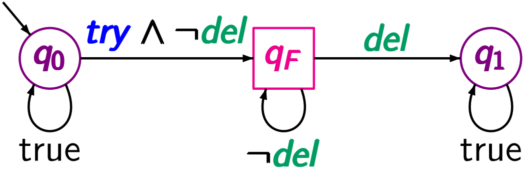
$\mathcal{T} \not\models \varphi$

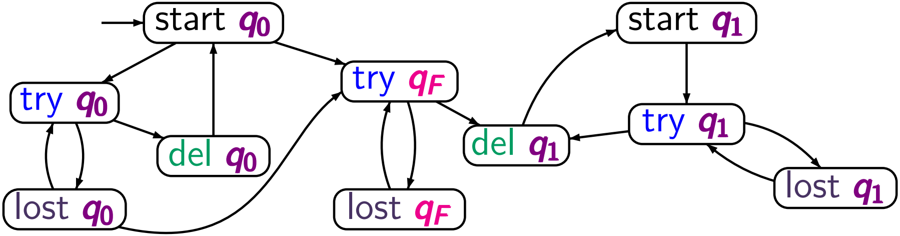
Example: LTL model checking

TS $\mathcal{T}$



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

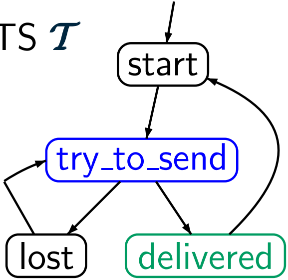




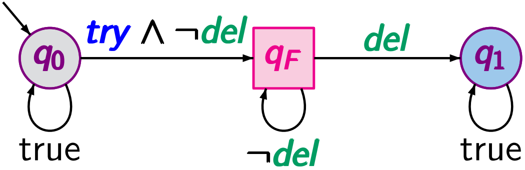
reachable fragment of the product-TS

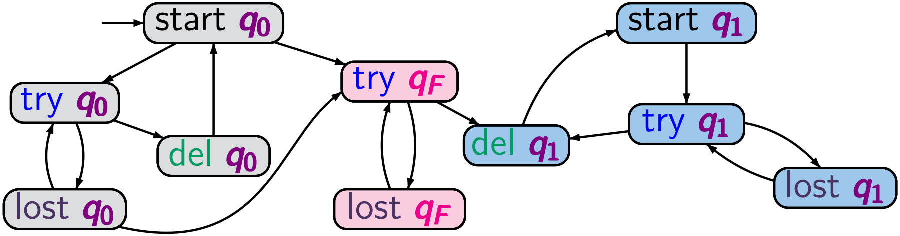
Example: LTL model checking

TS $\mathcal{T}$



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

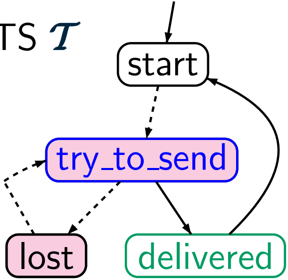




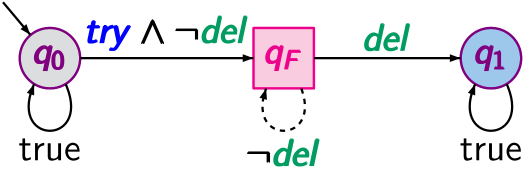
set of atomic propositions $AP' = \{q_0, q_1, q_F\}$

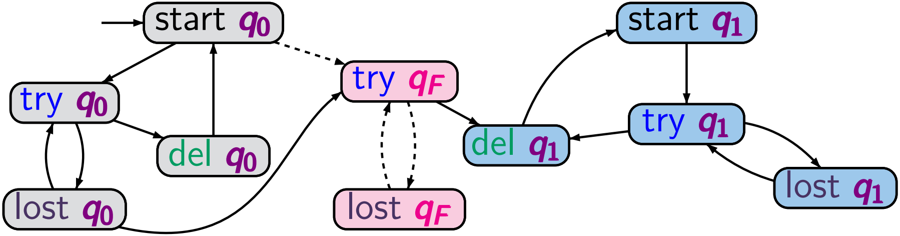
Example: LTL model checking

TS $\mathcal{T}$



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

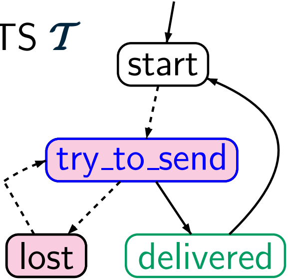




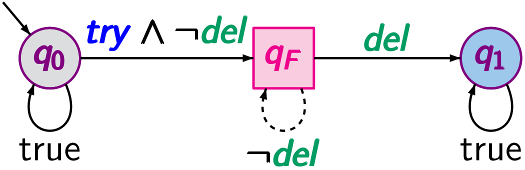
$$\mathcal{T} \otimes \mathcal{A} \not\models \Diamond\Box\neg F$$

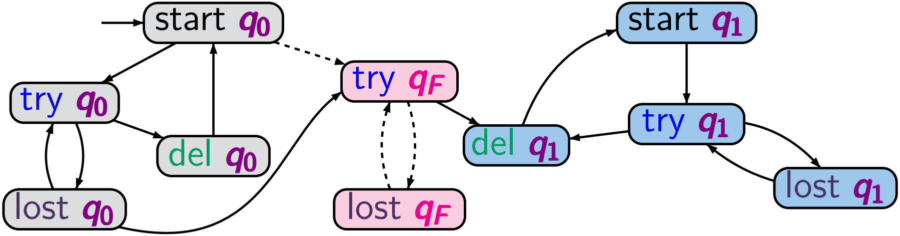
Example: LTL model checking

TS $\mathcal{T}$



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





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