LTL Model Checking

Lecture #3 of Principles of Model Checking

Joost-Pieter Katoen

Software Modeling and Verification Group

affiliated to University of Twente, Formal Methods and Tools

University of Twente, September 12, 2012

Content of this lecture

- Linear temporal logic
  - syntax, semantics, specifying properties
- Equivalences and fairness
  - weak until, fairness in LTL
- LTL model checking
  - GNBA, from LTL to GNBA, complexity

Content of this lecture

⇒ Linear temporal logic

- syntax, semantics, specifying properties

- Equivalences and fairness
  - weak until, fairness in LTL

- LTL model checking
  - GNBA, from LTL to GNBA, complexity

LT properties

- An LT property is a set of infinite traces over AP
- Specifying such sets explicitly is often inconvenient
- Mutual exclusion is specified over $AP = \{ c_1, c_2 \}$ by

$$P_{mutex} = \text{set of infinite words } A_0\, A_1\, A_2 \ldots \text{ with } \{ c_1, c_2 \} \not\subseteq A_i \text{ for all } 0 \leqslant i$$

- Starvation freedom is specified over $AP = \{ c_1, w_1, c_2, w_2 \}$ by

$$P_{nostarve} = \text{set of infinite words } A_0\, A_1\, A_2 \ldots \text{ such that:}$$

$$\left(\overset{\infty}{\exists}\, j.\ w_1 \in A_j\right) \Rightarrow \left(\overset{\infty}{\exists}\, j.\ c_1 \in A_j\right) \wedge \left(\overset{\infty}{\exists}\, j.\ w_2 \in A_j\right) \Rightarrow \left(\overset{\infty}{\exists}\, j.\ c_2 \in A_j\right)$$

such properties can be specified succinctly using logic

Linear Temporal Logic: Syntax

- Propositional logic
  - $a \in AP$ — atomic proposition
  - $\neg\phi$ and $\phi \wedge \psi$ — negation and conjunction
- Temporal operators
  - $\bigcirc \phi$ — neXt state fulfills ϕ
  - $\phi \,\mathsf{U}\, \psi$ — ϕ holds Until a ψ-state is reached

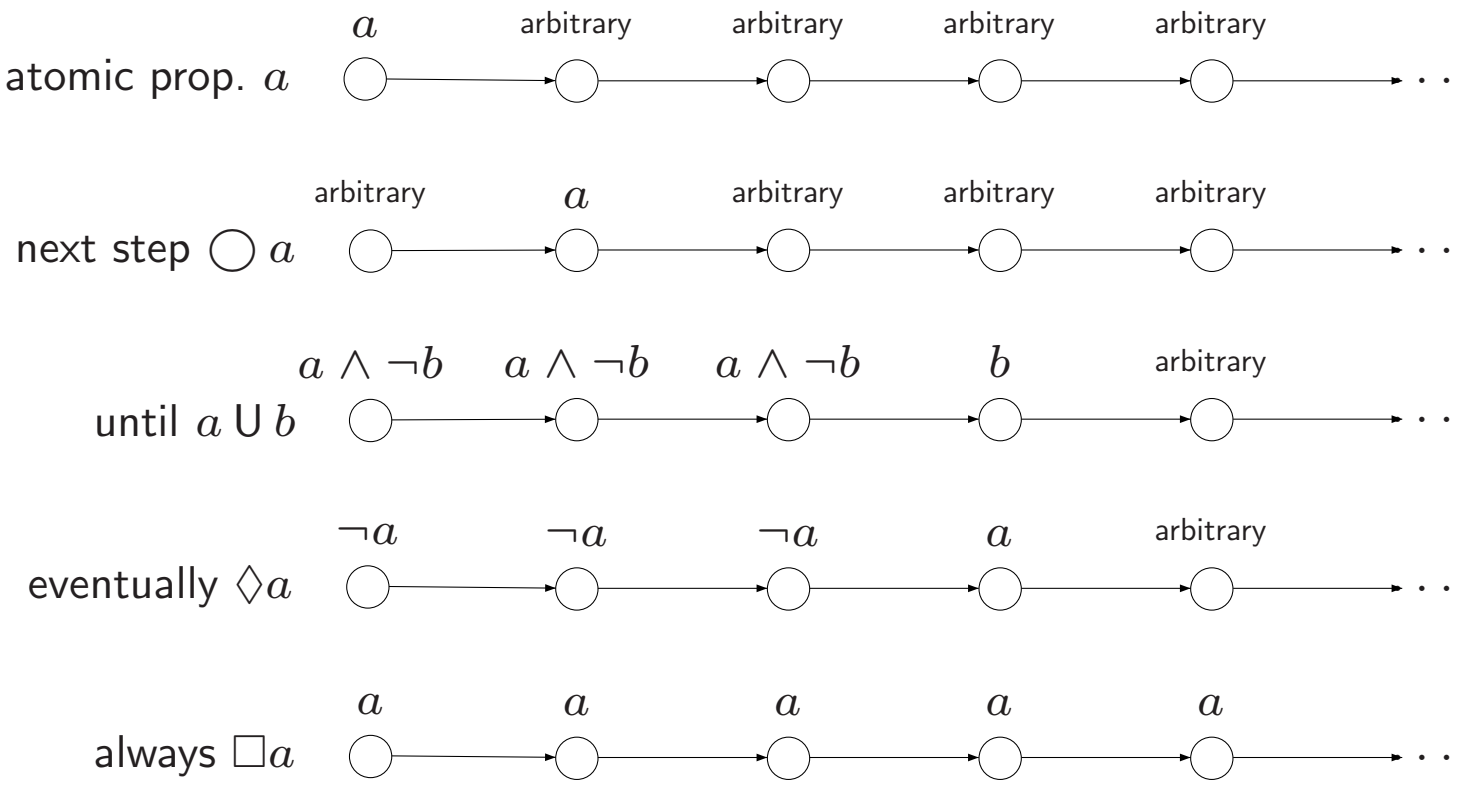
linear temporal logic is a logic for describing LT properties

Derived operators

$$
\begin{aligned}
\phi \vee \psi &\equiv \neg(\neg\phi \wedge \neg\psi) \\
\phi \Rightarrow \psi &\equiv \neg\phi \vee \psi \\
\phi \Leftrightarrow \psi &\equiv (\phi \Rightarrow \psi) \wedge (\psi \Rightarrow \phi) \\
\phi \oplus \psi &\equiv (\phi \wedge \neg\psi) \vee (\neg\phi \wedge \psi) \\
\mathsf{true} &\equiv \phi \vee \neg\phi \\
\mathsf{false} &\equiv \neg\,\mathsf{true} \\
\Diamond\,\phi &\equiv \mathsf{true}\,\mathsf{U}\,\phi \qquad \text{“sometimes in the future”} \\
\Box\,\phi &\equiv \neg\Diamond\neg\phi \qquad \text{“from now on for ever”}
\end{aligned}
$$

precedence order: the unary operators bind stronger than the binary ones.
$\neg$ and $\bigcirc$ bind equally strong. U takes precedence over $\wedge$, $\vee$, and $\rightarrow$

Intuitive semantics



LT properties

- Mutual exclusion is specified over $AP = \{ c_1, c_2 \}$ by

$$P_{mutex} \;=\; \text{set of infinite words } A_0\, A_1\, A_2 \ldots \text{ with } \{ c_1, c_2 \} \not\subseteq A_i \text{ for all } 0 \leqslant i$$

- In LTL: $\Box \neg (c_1 \wedge c_2)$

- Starvation freedom is specified over $AP = \{ c_1, w_1, c_2, w_2 \}$ by

$$P_{nostarve} = \text{ set of infinite words } A_0\, A_1\, A_2 \ldots \text{ such that:}$$

$$\left(\overset{\infty}{\exists}\, j.\; w_1 \in A_j\right) \Rightarrow \left(\overset{\infty}{\exists}\, j.\; c_1 \in A_j\right) \wedge \left(\overset{\infty}{\exists}\, j.\; w_2 \in A_j\right) \Rightarrow \left(\overset{\infty}{\exists}\, j.\; c_2 \in A_j\right)$$

- In LTL: $(\Box \Diamond w_1 \;\Rightarrow\; \Box \Diamond c_1) \;\wedge\; (\Box \Diamond w_2 \;\Rightarrow\; \Box \Diamond c_2)$

Semantics over words

The LT-property induced by LTL formula φ over AP is:

$$\mathit{Words}(\varphi) \;=\; \left\{\sigma \in \left(2^{AP}\right)^{\omega} \mid \sigma \models \varphi\right\}, \text{ where } \models \text{ is the smallest relation satisfying:}$$

$$\begin{array}{lcll}
\sigma & \models & \mathsf{true} & \\
\sigma & \models & a & \text{iff} \quad a \in A_0 \quad (\text{i.e., } A_0 \models a) \\
\sigma & \models & \varphi_1 \wedge \varphi_2 & \text{iff} \quad \sigma \models \varphi_1 \text{ and } \sigma \models \varphi_2 \\
\sigma & \models & \neg\, \varphi & \text{iff} \quad \sigma \not\models \varphi \\
\sigma & \models & \bigcirc \varphi & \text{iff} \quad \sigma[1..] = A_1 A_2 A_3 \ldots \models \varphi \\
\sigma & \models & \varphi_1 \,\mathsf{U}\, \varphi_2 & \text{iff} \quad \exists j \geqslant 0.\ \sigma[j..] \models \varphi_2 \ \text{ and } \ \sigma[i..] \models \varphi_1,\ 0 \leqslant i < j
\end{array}$$

for $\sigma = A_0 A_1 A_2 \ldots$ we have $\sigma[i..] = A_i A_{i+1} A_{i+2} \ldots$ is the suffix of σ from index i on

Semantics of $\Box$, $\Diamond$, $\Box\Diamond$ and $\Diamond\Box$

$$\sigma \models \Diamond\varphi \quad \text{iff} \quad \exists j \geqslant 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\varphi \quad \text{iff} \quad \forall j \geqslant 0.\ \sigma[j..] \models \varphi$$

$$\sigma \models \Box\Diamond\varphi \quad \text{iff} \quad \forall j \geqslant 0.\, \exists i \geqslant j.\ \sigma[i \ldots] \models \varphi$$

$$\sigma \models \Diamond\Box\varphi \quad \text{iff} \quad \exists j \geqslant 0.\, \forall i \geqslant j.\ \sigma[i \ldots] \models \varphi$$

Semantics over paths and states

Let $TS = (S, Act, \rightarrow, I, AP, L)$ and φ an LTL-formula over AP.

- For infinite path fragment π of TS:

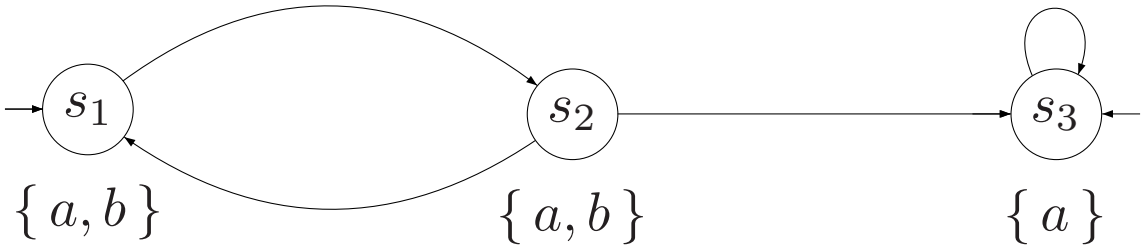
$$\pi \models \varphi \qquad \text{iff} \qquad trace(\pi) \models \varphi$$

- For state $s \in S$:

$$s \models \varphi \qquad \text{iff} \qquad \forall \pi \in Paths(s).\ \pi \models \varphi$$

- TS satisfies φ, denoted $TS \models \varphi$, iff $Traces(TS) \subseteq Words(\varphi)$

Example



$TS \models \Box a$

$TS \models \Box(\neg b \Rightarrow \Box(a \wedge \neg b))$

$TS \not\models \bigcirc(a \wedge b)$

$TS \not\models b \,\mathsf{U}\, (a \wedge \neg b)$

Practical properties in LTL

- Reachability
  - simple reachability $\Diamond \psi$
  - conditional reachability $\phi \, \mathsf{U} \, \psi$
- Safety
  - invariant $\Box \phi$
- Liveness $\Box (\phi \Rightarrow \Diamond \psi)$ and others
- Fairness $\Box \Diamond \phi$ and others

Semantics of negation

For paths, it holds $\pi \models \varphi$ if and only if $\pi \not\models \neg\varphi$ since:

$$\mathit{Words}(\neg\varphi) = \left(2^{AP}\right)^{\omega} \setminus \mathit{Words}(\varphi) \quad .$$

But: $\mathit{TS} \not\models \varphi$ and $\mathit{TS} \models \neg\varphi$ are *not* equivalent in general

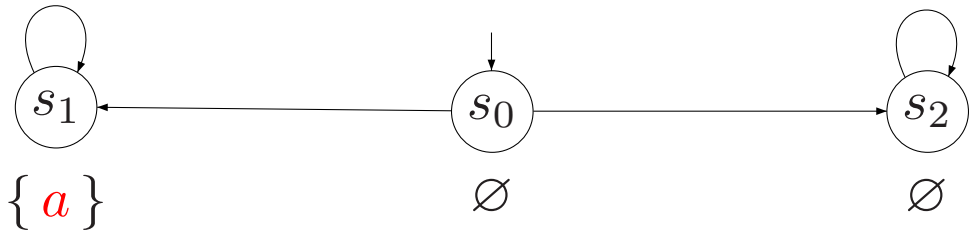
It holds: $\mathit{TS} \models \neg\varphi$ implies $\mathit{TS} \not\models \varphi$. Not always the reverse!

Note that:

$$\begin{aligned} \mathit{TS} \not\models \varphi \quad & \text{iff } \mathit{Traces}(\mathit{TS}) \not\subseteq \mathit{Words}(\varphi) \\ & \text{iff } \mathit{Traces}(\mathit{TS}) \setminus \mathit{Words}(\varphi) \neq \varnothing \\ & \text{iff } \mathit{Traces}(\mathit{TS}) \cap \mathit{Words}(\neg\varphi) \neq \varnothing \quad . \end{aligned}$$

TS neither satisfies φ nor $\neg\varphi$ if there are
paths π_1 and π_2 in TS such that $\pi_1 \models \varphi$ and $\pi_2 \models \neg\varphi$

Example



A transition system for which $TS \not\models \Diamond a$ and $TS \not\models \neg\Diamond a$

Content of this lecture

- Linear temporal logic
  - syntax, semantics, specifying properties

$\Rightarrow$ Equivalences and fairness
  - weak until, fairness in LTL

- LTL model checking
  - GNBA, from LTL to GNBA, complexity

Equivalence

LTL formulas ϕ, ψ are *equivalent*, denoted $\phi \equiv \psi$, if:

$$\mathit{Words}(\phi) = \mathit{Words}(\psi)$$

Duality and idempotence laws

Duality:

$$\neg \Box \phi \equiv \Diamond \neg \phi$$
$$\neg \Diamond \phi \equiv \Box \neg \phi$$
$$\neg \bigcirc \phi \equiv \bigcirc \neg \phi$$

Idempotency:

$$\Box \Box \phi \equiv \Box \phi$$
$$\Diamond \Diamond \phi \equiv \Diamond \phi$$
$$\phi \,\mathsf{U}\, (\phi \,\mathsf{U}\, \psi) \equiv \phi \,\mathsf{U}\, \psi$$
$$(\phi \,\mathsf{U}\, \psi) \,\mathsf{U}\, \psi \equiv \phi \,\mathsf{U}\, \psi$$

Absorption and distributive laws

Absorption:

$$\Diamond\Box\Diamond\phi \equiv \Box\Diamond\phi$$

$$\Box\Diamond\Box\phi \equiv \Diamond\Box\phi$$

Distribution:

$$\bigcirc(\phi \,\mathsf{U}\, \psi) \equiv (\bigcirc\phi)\,\mathsf{U}\,(\bigcirc\psi)$$

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

$$\Box(\phi \wedge \psi) \equiv \Box\phi \wedge \Box\psi$$

but .....:

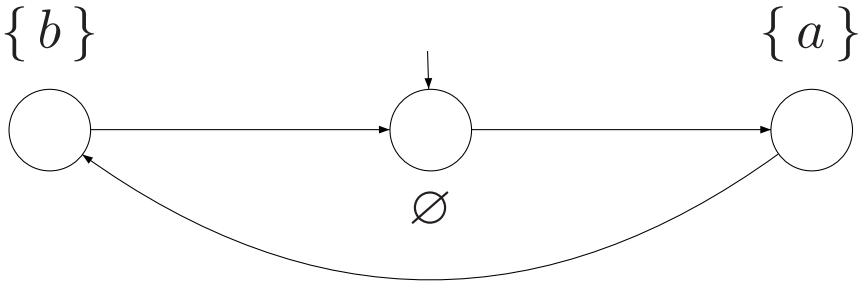
$$\Diamond(\phi \,\mathsf{U}\, \psi) \not\equiv (\Diamond\phi)\,\mathsf{U}\,(\Diamond\psi)$$

$$\Diamond(\phi \wedge \psi) \not\equiv \Diamond\phi \wedge \Diamond\psi$$

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

Distributive laws

$$\Diamond(a \wedge b) \not\equiv \Diamond a \wedge \Diamond b \quad \text{and} \quad \Box(a \vee b) \not\equiv \Box a \vee \Box b$$



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

Expansion laws

Expansion:
$$\phi \,\mathsf{U}\, \psi \equiv \psi \vee (\phi \wedge \bigcirc(\phi \,\mathsf{U}\, \psi))$$
$$\Diamond \phi \equiv \phi \vee \bigcirc \Diamond \phi$$
$$\Box \phi \equiv \phi \wedge \bigcirc \Box \phi$$

proof on the black board

Expansion for until

$P = \mathit{Words}(\varphi \,\mathsf{U}\, \psi)$ satisfies:

$$P \;=\; \mathit{Words}(\psi) \cup \big\{\, A_0A_1A_2\ldots \in \mathit{Words}(\varphi) \;\mid\; A_1A_2\ldots \in P \,\big\}$$

and is the *smallest* LT-property such that:

$$\mathit{Words}(\psi) \cup \big\{A_0A_1A_2\ldots \in \mathit{Words}(\varphi) \;\mid\; A_1A_2\ldots \in P\big\} \;\subseteq\; P \quad (*)$$

smallest LT-property satisfying condition (*) means that:
$P = \mathit{Words}(\varphi \,\mathsf{U}\, \psi)$ satisfies (*) and $\mathit{Words}(\varphi \,\mathsf{U}\, \psi) \subseteq P$ for each P satisfying (*)

Weak until

- The *weak-until* (or: unless) operator: $\varphi \,\mathsf{W}\, \psi \stackrel{\text{def}}{=} (\varphi \,\mathsf{U}\, \psi) \vee \Box\varphi$
  - as opposed to until, $\varphi \,\mathsf{W}\, \psi$ does not require a ψ-state to be reached
- Until U and weak until W are *dual*:

$$\begin{aligned} \neg(\varphi \,\mathsf{U}\, \psi) &\equiv (\varphi \wedge \neg\psi) \,\mathsf{W}\, (\neg\varphi \wedge \neg\psi) \\ \neg(\varphi \,\mathsf{W}\, \psi) &\equiv (\varphi \wedge \neg\psi) \,\mathsf{U}\, (\neg\varphi \wedge \neg\psi) \end{aligned}$$

- Until and weak until are *equally expressive*:
  - $\Box\psi \equiv \psi \,\mathsf{W}\, \mathsf{false}$ and $\varphi \,\mathsf{U}\, \psi \equiv (\varphi \,\mathsf{W}\, \psi) \wedge \neg\Box\neg\psi$
- Until and weak until satisfy the *same expansion law*
  - but until is the smallest, and weak until the largest solution!

Expansion for weak until

$P = \mathit{Words}(\varphi \,\mathsf{W}\, \psi)$ satisfies:

$$P \;=\; \mathit{Words}(\psi) \cup \big\{\, A_0A_1A_2\ldots \in \mathit{Words}(\varphi) \;\mid\; A_1A_2\ldots \in P \,\big\}$$

and is the *largest* LT-property such that:

$$\mathit{Words}(\psi) \cup \big\{A_0A_1A_2\ldots \in \mathit{Words}(\varphi) \;\mid\; A_1A_2\ldots \in P\big\} \;\supseteq\; P \quad (**)$$

largest LT-property satisfying condition (**) means that:
$P \supseteq \mathit{Words}(\varphi \,\mathsf{W}\, \psi)$ satisfies (**) and $\mathit{Words}(\varphi \,\mathsf{W}\, \psi) \supseteq P$ for each P satisfying (**)

LTL fairness constraints

Let Φ and Ψ be propositional logic formulas over *AP*.

1. An *unconditional LTL fairness constraint* is of the form:

$$ufair \;=\; \Box\Diamond\Psi$$

2. A *strong LTL fairness condition* is of the form:

$$sfair \;=\; \Box\Diamond\Phi \;\longrightarrow\; \Box\Diamond\Psi$$

3. A *weak LTL fairness constraint* is of the form:

$$wfair \;=\; \Diamond\Box\Phi \;\longrightarrow\; \Box\Diamond\Psi$$

Φ stands for "something is enabled"; Ψ for "something is taken"

LTL fairness assumption

- *LTL fairness assumption* = conjunction of LTL fairness constraints
  - the fairness constraints are of any arbitrary type
- Strong fairness assumption: $sfair = \bigwedge_{0<i\leqslant k} \left(\Box\Diamond\Phi_i \longrightarrow \Box\Diamond\Psi_i\right)$
  - compare this to an action-based strong fairness constraint over A with $|A| = k$
- General format: $fair = ufair \wedge sfair \wedge wfair$
- Rules of thumb:
  - strong (or unconditional) fairness assumptions are useful for solving contentions
  - weak fairness suffices for resolving nondeterminism resulting from interleaving

Fair satisfaction

For state s in transition system TS (over AP) without terminal states, let

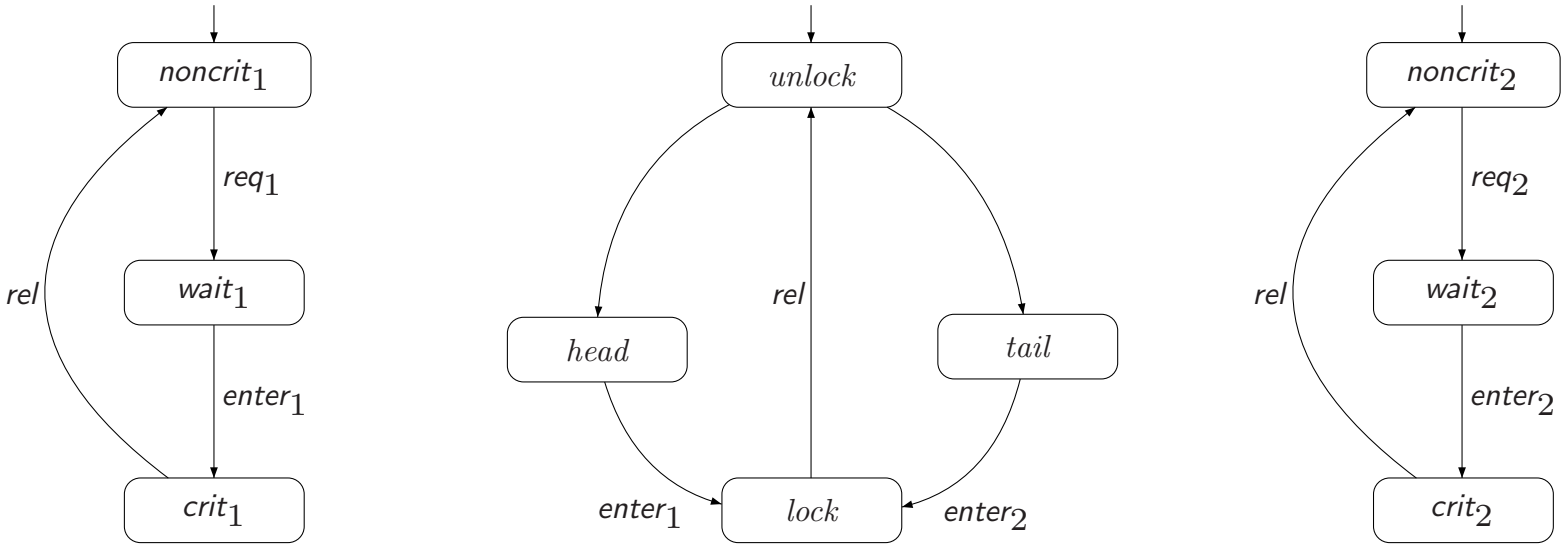
$$\begin{aligned} \mathit{FairPaths}_{fair}(s) &= \left\{ \pi \in \mathit{Paths}(s) \mid \pi \models fair \right\} \\ \mathit{FairTraces}_{fair}(s) &= \left\{ \mathit{trace}(\pi) \mid \pi \in \mathit{FairPaths}_{fair}(s) \right\} \end{aligned}$$

For LTL-formula φ, and LTL fairness assumption $fair$:

$$\begin{aligned} s \models_{fair} \varphi \quad &\text{if and only if} \quad \forall \pi \in \mathit{FairPaths}_{fair}(s).\, \pi \models \varphi \quad \text{and} \\ TS \models_{fair} \varphi \quad &\text{if and only if} \quad \forall s_0 \in I.\, s_0 \models_{fair} \varphi \end{aligned}$$

$\models_{fair}$ is the *fair satisfaction relation* for LTL; $\models$ the standard one for LTL

Randomized arbiter



$$TS_1 \parallel Arbiter \parallel TS_2 \not\models \Box\Diamond\, crit_1$$

But: $TS_1 \parallel Arbiter \parallel TS_2 \models_{fair} \Box\Diamond crit_1 \wedge \Box\Diamond crit_2$ with $fair = \Box\Diamond head \wedge \Box\Diamond tail$

Reducing $\models_{fair}$ to $\models$

For:

- transition system TS without terminal states
- LTL formula φ, and
- LTL fairness assumption $fair$

it holds:

$$TS \models_{fair} \varphi \quad \text{if and only if} \quad TS \models (fair \rightarrow \varphi)$$

verifying an LTL-formula under a fairness assumption can be done using standard verification algorithms for LTL

Content of this lecture

- Linear temporal logic
  - syntax, semantics, specifying properties
- Equivalences and fairness
  - weak until, fairness in LTL

$\Rightarrow$ LTL model checking

  - GNBA, from LTL to GNBA, complexity

LTL model-checking problem

The following decision problem:

Given finite transition system TS and LTL-formula φ:

yields "yes" if $TS \models \varphi$, and "no" (plus a counterexample) if $TS \not\models \varphi$

NBA for LTL-formulae

A first attempt

$$TS \models \varphi \quad \text{if and only if} \quad \mathit{Traces}(TS) \subseteq \underbrace{\mathit{Words}(\varphi)}_{\mathcal{L}_\omega(\mathcal{A}_\varphi)}$$

$$\text{if and only if} \quad \mathit{Traces}(TS) \cap \overline{\mathcal{L}_\omega(\mathcal{A}_\varphi)} = \varnothing$$

$$\text{if and only if} \quad \mathit{Traces}(TS) \cap \mathcal{L}_\omega(\overline{\mathcal{A}_\varphi}) = \varnothing$$

but complementation of NBA is quadratically exponential

if $\mathcal{A}$ has n states, $\overline{\mathcal{A}}$ has c^{n^2} states in worst case

Observation

$TS \models \varphi$ if and only if $\mathit{Traces}(TS) \subseteq \mathit{Words}(\varphi)$

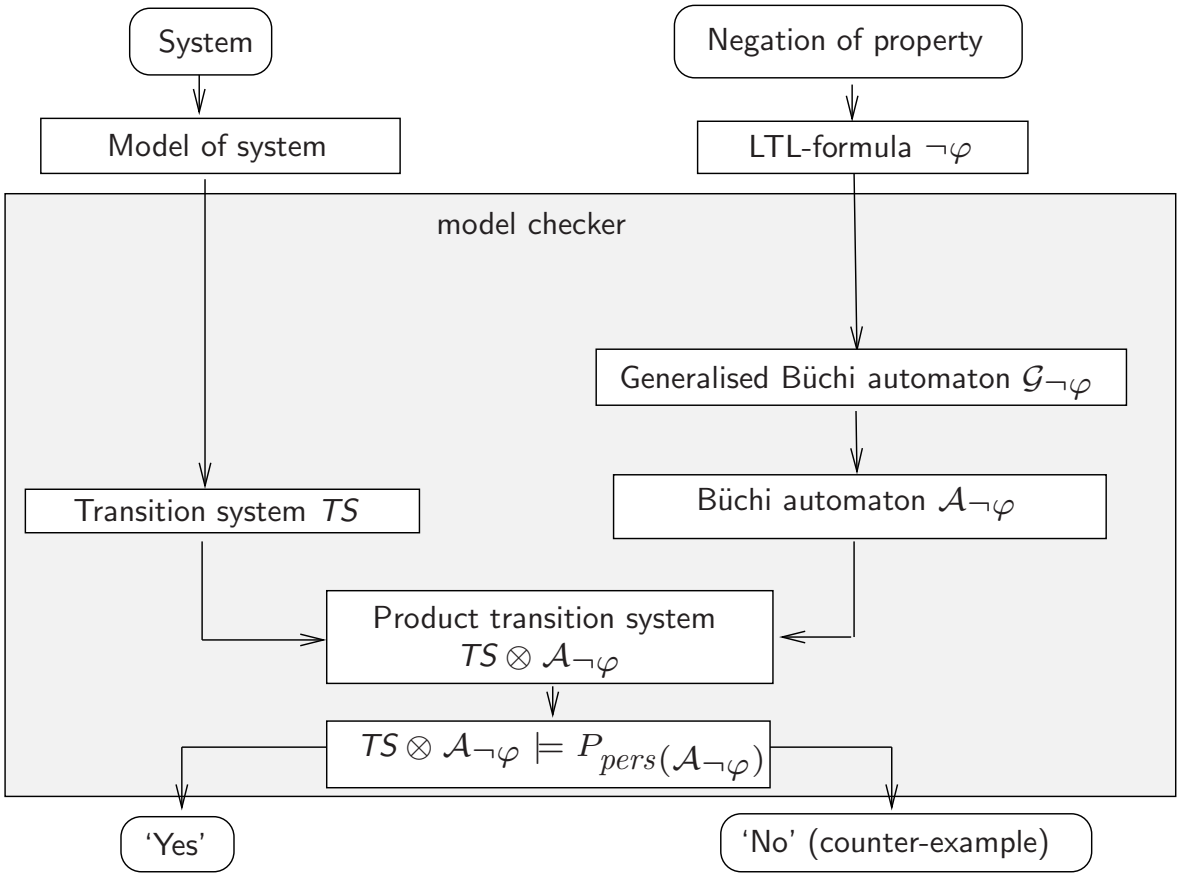
if and only if $\mathit{Traces}(TS) \cap \big((2^{AP})^\omega \setminus \mathit{Words}(\varphi)\big) = \varnothing$

if and only if $\mathit{Traces}(TS) \cap \underbrace{\mathit{Words}(\neg\varphi)}_{\mathcal{L}_\omega(\mathcal{A}_{\neg\varphi})} = \varnothing$

if and only if $TS \otimes \mathcal{A}_{\neg\varphi} \models \Diamond\Box\, \neg F$

LTL model checking is thus reduced to persistence checking!

Overview of LTL model checking



Generalized Büchi automata

- NBA are as expressive as ω-regular languages
- Variants of NBA exist that are equally expressive
  - Muller, Rabin, Streett automata, and eneralized Büchi automata (GNBA)
- GNBA are like NBA, but have a distinct acceptance criterion
  - a GNBA requires to visit several sets $F_1, \ldots, F_k$ $(k \geqslant 0)$ infinitely often
  - for $k{=}0$, all runs are accepting; for $k{=}1$ it behaves like an NBA
- GNBA are useful to relate temporal logic and automata

Generalized Büchi automata

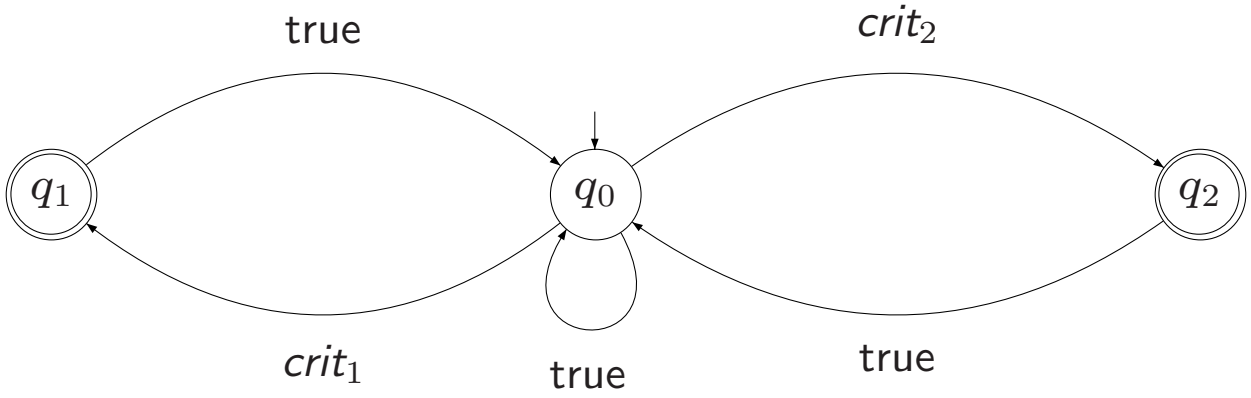
A generalized NBA (GNBA) $\mathcal{G}$ is a tuple $(Q, \Sigma, \delta, Q_0, \mathcal{F})$ where:

- Q, Σ, δ and Q_0 are as before, and
- $\mathcal{F} = \{ F_1, \ldots, F_k \}$ is a (possibly empty) subset of 2^Q

Language of a GNBA

- GNBA $\mathcal{G} = (Q, \Sigma, \delta, Q_0, \mathcal{F})$ and word $\sigma = A_0 A_1 A_2 \ldots \in \Sigma^\omega$
- A accepted run for σ in $\mathcal{G}$ is an infinite sequence $q_0\, q_1\, q_2 \ldots$ such that:
  - $q_0 \in Q_0$ and $q_i \xrightarrow{A_i} q_{i+1}$ for all $0 \leqslant i$, and
  - for all $F \in \mathcal{F}$: $q_i \in F$ for infinitely many i
- $\mathcal{L}_\omega(\mathcal{G}) = \{\sigma \in \Sigma^\omega \mid$ there exists an accepting run for σ in $\mathcal{G}\}$

Example



A GNBA for the property "both processes are infinitely often in their critical section"

$$\mathcal{F} = \{ \{ q_1 \}, \{ q_2 \} \}$$

From GNBA to NBA

For any GNBA $\mathcal{G}$ there exists an NBA $\mathcal{A}$ with:

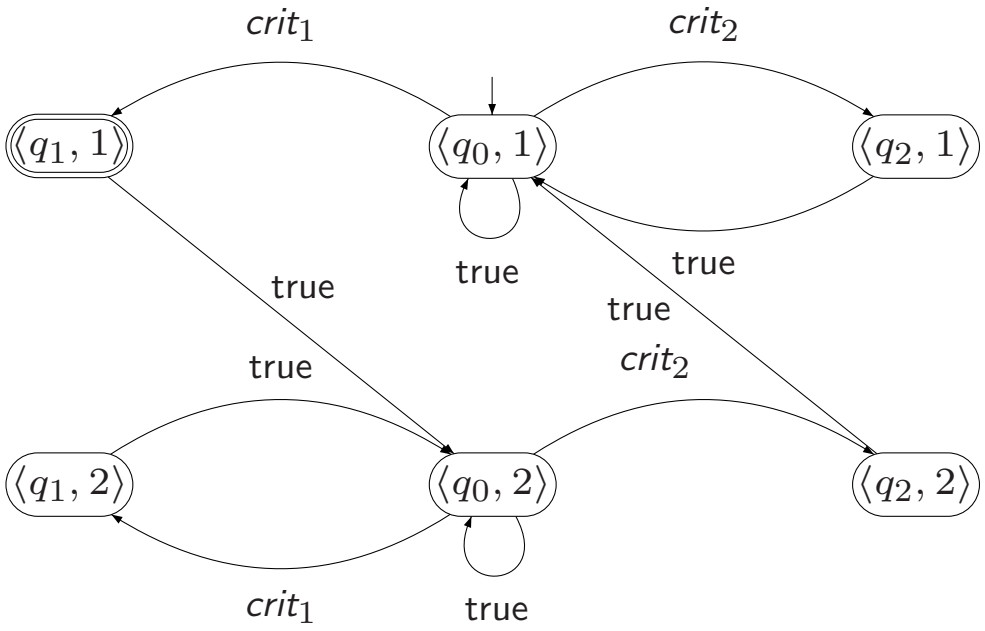
$\mathcal{L}_\omega(\mathcal{G}) = \mathcal{L}_\omega(\mathcal{A})$ and $|\mathcal{A}| = \mathcal{O}(|\mathcal{G}| \cdot |\mathcal{F}|)$

where $\mathcal{F}$ denotes the set of acceptance sets in $\mathcal{G}$

Sketch of transformation GNBA (with $|\mathcal{F}| = k$) into equivalent NBA:

- make k copies of the GNBA
- initial states of NBA := the initial states in the first copy
- final states of NBA := accept set F_1 in the first copy
- on visiting in i-th copy a state in F_i, then move to the $(i{+}1)$-st copy

Example


$crit_1$
$crit_2$
$\langle q_1, 1\rangle$
$\langle q_0, 1\rangle$
$\langle q_2, 1\rangle$
true
true
true
true
$crit_2$
true
$\langle q_1, 2\rangle$
$\langle q_0, 2\rangle$
$\langle q_2, 2\rangle$
$crit_1$
true

From LTL to GNBA

GNBA $\mathcal{G}_\varphi$ over 2^{AP} for LTL-formula φ with $\mathcal{L}_\omega(\mathcal{G}_\varphi) = \mathit{Words}(\varphi)$:

- Assume φ only contains the operators $\wedge$, $\neg$, $\bigcirc$ and U
- States are elementary sets of sub-formulas in φ
  - for $\sigma = A_0 A_1 A_2 \ldots \in \mathit{Words}(\varphi)$, "expand" $A_i \subseteq AP$ with sub-formulas of φ
  - ... to obtain $\bar{\sigma} = B_0 B_1 B_2 \ldots$ such that

$$\psi \in B_i \qquad \text{if and only if} \qquad \sigma^i = A_i A_{i+1} A_{i+2} \ldots \models \psi$$

  - $\bar{\sigma}$ is intended to be a run in GNBA $\mathcal{G}_\varphi$ for σ
- Transitions are derived from semantics $\bigcirc$ and expansion law for U
- Accept sets guarantee that: $\bar{\sigma}$ is an accepting run for σ iff $\sigma \models \varphi$

From LTL to GNBA: the states (example)

- Let $\varphi = a \,\mathsf{U}\, (\neg a \wedge b)$ and $\sigma = \{a\}\{a,b\}\{b\}\ldots$
  - B_i is a subset of $\{a, b, \neg a \wedge b, \varphi\} \cup \{\neg a, \neg b, \neg(\neg a \wedge b), \neg\varphi\}$
  - this set of formulas is also called the *closure* of φ

- Extend $A_0 = \{a\}$, $A_1 = \{a,b\}$, $A_2 = \{b\}$, ... as follows:
  - extend A_0 with $\neg b$, $\neg(\neg a \wedge b)$, and φ as they hold in $\sigma^0 = \sigma$ (and no others)
  - extend A_1 with $\neg(\neg a \wedge b)$ and φ as they hold in σ^1 (and no others)
  - extend A_2 with $\neg a$, $\neg a \wedge b$ and φ as they hold in σ^2 (and no others)
  - ... and so forth
  - this is not effective and is performed on the automaton (not on words)

- Result:
  - $\bar{\sigma} = \underbrace{\{a, \neg b, \neg(\neg a \wedge b), \varphi\}}_{B_0} \underbrace{\{a, b, \neg(\neg a \wedge b), \varphi\}}_{B_1} \underbrace{\{\neg a, b, \neg a \wedge b, \varphi\}}_{B_2} \ldots$

Closure

For LTL-formula φ, the set *closure*(φ)

consists of all sub-formulas ψ of φ and their negation $\neg\psi$

(where ψ and $\neg\neg\psi$ are identified)

for $\varphi = a \,\mathsf{U}\, (\neg a \wedge b)$, *closure*($\varphi$) $= \{\, a, b, \neg a, \neg b, \neg a \wedge b, \neg(\neg a \wedge b), \varphi, \neg\varphi \,\}$

can we take B_i as any subset of *closure*(φ)? no! they must be elementary

Elementary sets of formulae

$B \subseteq \mathit{closure}(\varphi)$ is *elementary* if:

1. B is *logically consistent* if for all $\varphi_1 \wedge \varphi_2, \psi \in \mathit{closure}(\varphi)$:
   - $\varphi_1 \wedge \varphi_2 \in B \;\Leftrightarrow\; \varphi_1 \in B$ and $\varphi_2 \in B$
   - $\psi \in B \;\Rightarrow\; \neg\psi \notin B$
   - true $\in \mathit{closure}(\varphi) \;\Rightarrow\;$ true $\in B$

2. B is *locally consistent* if for all $\varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathit{closure}(\varphi)$:
   - $\varphi_2 \in B \;\Rightarrow\; \varphi_1 \,\mathsf{U}\, \varphi_2 \in B$
   - $\varphi_1 \,\mathsf{U}\, \varphi_2 \in B$ and $\varphi_2 \notin B \;\Rightarrow\; \varphi_1 \in B$

3. B is *maximal*, i.e., for all $\psi \in \mathit{closure}(\varphi)$:
   - $\psi \notin B \;\Rightarrow\; \neg\psi \in B$

Examples

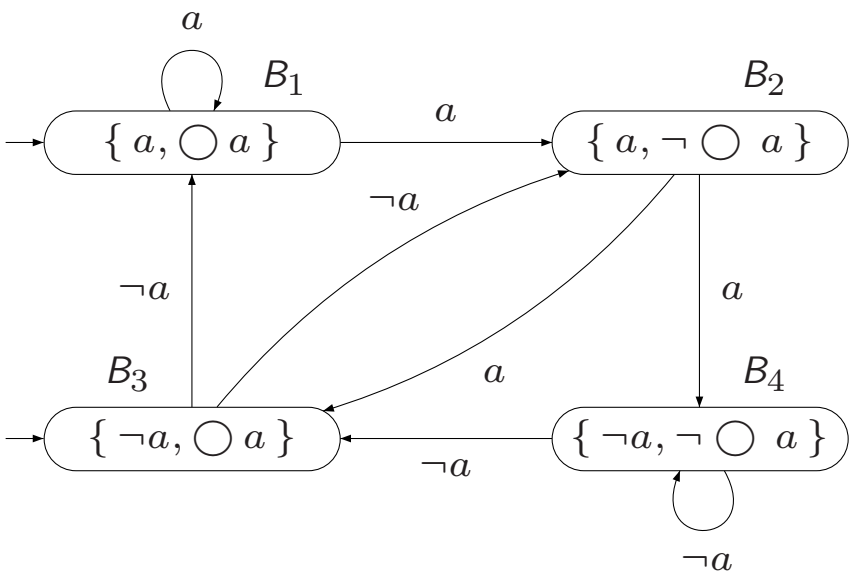
The GNBA of LTL-formula φ

For LTL-formula φ, let $\mathcal{G}_\varphi = (Q, 2^{AP}, \delta, Q_0, \mathcal{F})$ where

- $Q =$ all elementary sets $B \subseteq \mathit{closure}(\varphi)$, $Q_0 = \{ B \in Q \mid \varphi \in B \}$
- $\mathcal{F} = \Big\{ \{ B \in Q \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \notin B \text{ or } \varphi_2 \in B \} \mid \varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathit{closure}(\varphi) \Big\}$
- The transition relation $\delta : Q \times 2^{AP} \to 2^Q$ is given by:
  - If $A \neq B \cap AP$ then $\delta(B, A) = \varnothing$
  - $\delta(B, B \cap AP)$ is the set B' of all elementary sets of formulas satisfying:
    (i) For every $\bigcirc \psi \in \mathit{closure}(\varphi)$: $\bigcirc \psi \in B \quad \Leftrightarrow \quad \psi \in B'$, and
    (ii) For every $\varphi_1 \,\mathsf{U}\, \varphi_2 \in \mathit{closure}(\varphi)$:

$$\varphi_1 \,\mathsf{U}\, \varphi_2 \in B \quad \Leftrightarrow \quad \Big(\varphi_2 \in B \;\vee\; (\varphi_1 \in B \;\wedge\; \varphi_1 \,\mathsf{U}\, \varphi_2 \in B') \Big)$$

GNBA for LTL-formula $\bigcirc a$



$Q_0 = \{ B_1, B_3 \}$ since $\bigcirc a \in B_1$ and $\bigcirc a \in B_3$

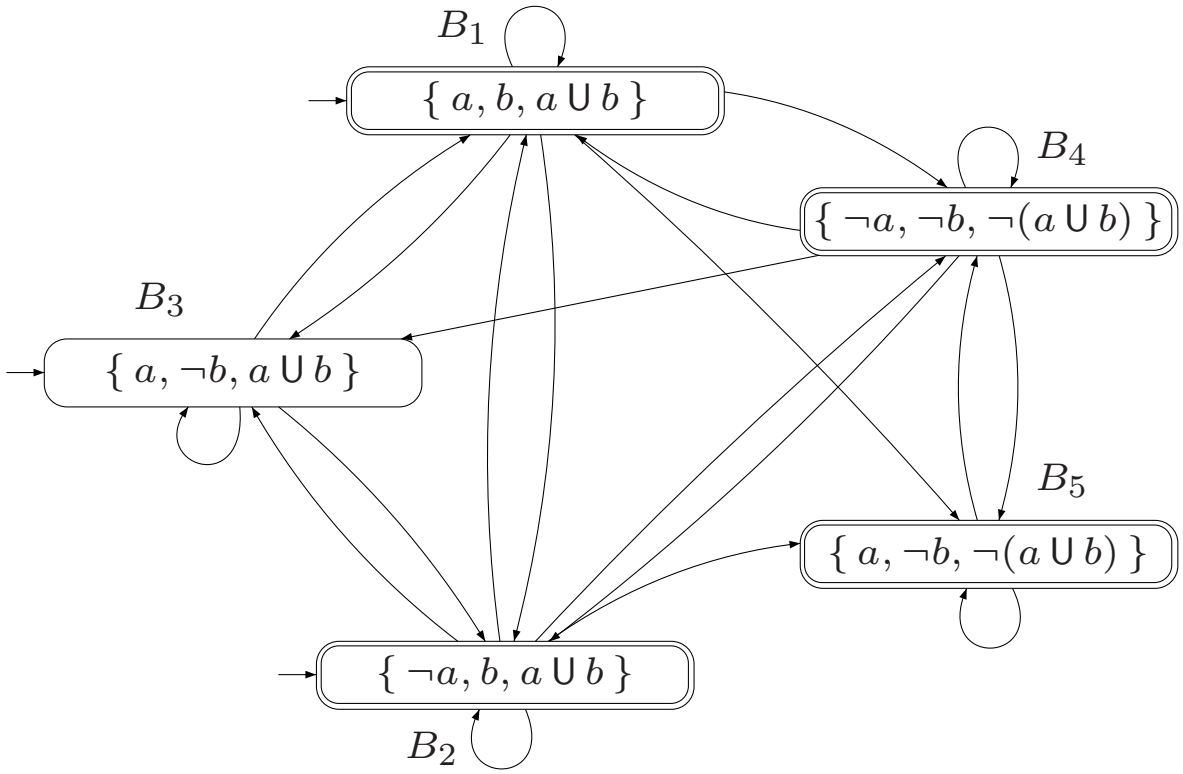
$\delta(B_2, \{ a \}) = \{ B_3, B_4 \}$ as $B_2 \cap \{ a \} = \{ a \}$, $\neg \bigcirc a = \bigcirc \neg a \in B_2$, and $\neg a \in B_3, B_4$

$\delta(B_1, \{ a \}) = \{ B_1, B_2 \}$ as $B_1 \cap \{ a \} = \{ a \}$, $\bigcirc a \in B_1$ and $a \in B_1, B_2$

$\delta(B_4, \{ a \}) = \varnothing$ since $B_4 \cap \{ a \} = \varnothing \neq \{ a \}$

The set $\mathcal{F}$ is empty, since $\varphi = \bigcirc a$ does not contain an until-operator

GNBA for LTL-formula $a \mathsf{U} b$



justification: on the black board

NBA are more expressive than LTL

Corollary: every LTL-formula expresses an ω-regular property

But: there exist ω-regular properties that cannot be expressed in LTL

Example: there is no LTL formula φ with $\mathit{Words}(\varphi) = P$ for the LT-property:

$$P = \left\{ A_0 A_1 A_2 \ldots \in \left(2^{\{a\}}\right)^\omega \mid a \in A_{2i} \text{ for } i \geqslant 0 \right\}$$

But there exists an NBA $\mathcal{A}$ with $\mathcal{L}_\omega(\mathcal{A}) = P$

$\Rightarrow$ *there are ω-regular properties that cannot be expressed in LTL!*

Complexity for LTL to NBA

For any LTL-formula φ (over AP) there exists an NBA $\mathcal{A}_\varphi$
with $\mathit{Words}(\varphi) = \mathcal{L}_\omega(\mathcal{A}_\varphi)$ and
which can be constructed in time and space in $2^{\mathcal{O}(|\varphi| \cdot \log |\varphi|)}$

Justification complexity: next slide

Time and space complexity

- States GNBA $\mathcal{G}_\varphi$ are elementary sets of formulae in *closure*(φ)
  - sets B can be represented by bit vectors with single bit per subformula ψ of φ
- The number of states in $\mathcal{G}_\varphi$ is bounded by $2^{|\mathsf{subf}(\varphi)|}$
  - where $\mathsf{subf}(\varphi)$ denotes the set of all subformulae of φ
  - $|\mathsf{subf}(\varphi)| \leqslant 2{\cdot}|\varphi|$; so, the number of states in $\mathcal{G}_\varphi$ is bounded by $2^{\mathcal{O}(|\varphi|)}$
- The number of accepting sets of $\mathcal{G}_\varphi$ is bounded above by $\mathcal{O}(|\varphi|)$
- The number of states in NBA $\mathcal{A}_\varphi$ is thus bounded by $2^{\mathcal{O}(|\varphi|)} \cdot \mathcal{O}(|\varphi|)$
- $2^{\mathcal{O}(|\varphi|)} \cdot \mathcal{O}(|\varphi|) \;=\; 2^{\mathcal{O}(|\varphi| \log |\varphi|)}$ qed

Lower bound

There exists a family of LTL formulas φ_n with $|\varphi_n| = \mathcal{O}(poly(n))$
such that every NBA $\mathcal{A}_{\varphi n}$ for φ_n has at least 2^n states

Proof (1)

Let AP be non-empty, that is, $|2^{AP}| \geqslant 2$ and:

$$\mathcal{L}_n \;=\; \Big\{\, A_1 \ldots A_n\, A_1 \ldots A_n\, \sigma \mid A_i \subseteq AP \wedge \sigma \in \Big(2^{AP}\Big)^{\omega} \,\Big\}, \qquad \text{for } n \geqslant 0$$

It follows $\mathcal{L}_n \;=\; \mathit{Words}(\varphi_n)$ where $\varphi_n \;=\; \bigwedge_{a \in AP} \bigwedge_{0 \leqslant i < n} (\bigcirc^i a \longleftrightarrow \bigcirc^{n+i} a)$

φ_n is an LTL formula of polynomial length: $|\varphi_n| \;\in\; \mathcal{O}\Big(|AP| \cdot n\Big)$

However, any NBA $\mathcal{A}$ with $\mathcal{L}_\omega(\mathcal{A}) = \mathcal{L}_n$ has at least 2^n states

Proof (2)

Claim: any NBA $\mathcal{A}$ for $\bigwedge_{a \in AP} \bigwedge_{0 \leqslant i < n} (\bigcirc^i a \longleftrightarrow \bigcirc^{n+i} a)$ has at least 2^n states

Words of the form $A_1 \ldots A_n \, A_1 \ldots A_n \, \varnothing \, \varnothing \, \varnothing \ldots$ are accepted by $\mathcal{A}$

$\mathcal{A}$ thus has for every word $A_1 \ldots A_n$ of length n, a state $q(A_1 \ldots A_n)$, say, which can be reached from an initial state by consuming $A_1 \ldots A_n$

From $q(A_1 \ldots A_n)$, it is possible to visit an accept state infinitely often by accepting the suffix $A_1 \ldots A_n \, \varnothing \, \varnothing \, \varnothing \ldots$

If $A_1 \ldots A_n \neq A'_1 \ldots A'_n$ then

$$A_1 \ldots A_n \, A'_1 \ldots A'_n \, \varnothing \, \varnothing \, \varnothing \ldots \notin \mathcal{L}_n = \mathcal{L}_\omega(\mathcal{A})$$

Therefore, the states $q(A_1 \ldots A_n)$ are all pairwise different

Given $|2^{AP}|$ possible sequences $A_1 \ldots A_n$, NBA $\mathcal{A}$ has $\geqslant \left(\left|2^{AP}\right|\right)^n \geqslant 2^n$ states

Complexity for LTL model checking

The time and space complexity of LTL model checking is in $\mathcal{O}\left(|TS| \cdot 2^{|\varphi|}\right)$

Theoretical complexity

The LTL model-checking problem is PSPACE-complete