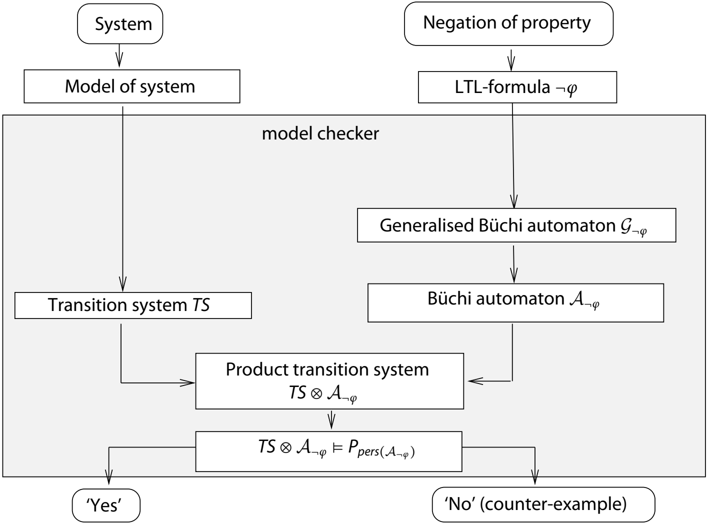
Verification

Lecture 8

Bernd Finkbeiner
Peter Faymonville
Michael Gerke

UNIVERSITÄT
DES
SAARLANDES

REVIEW: Overview of LTL model checking



REVIEW: Generalized Büchi automata

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

- Q is a finite set of states with $Q_0 \subseteq Q$ a set of initial states
- Σ is an alphabet
- $\delta : Q \times \Sigma \rightarrow 2^Q$ is a transition function
- $\mathcal{F} = \{ F_1, \ldots, F_k \}$ is a (possibly empty) subset of 2^Q

The size of $\mathcal{G}$, denoted $|\mathcal{G}|$, is the number of states and transitions in $\mathcal{G}$:

$$|\mathcal{G}| = |Q| + \sum_{q \in Q} \sum_{A \in \Sigma} |\, \delta(q, A) \,|$$

REVIEW: 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 *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 $0 \leq i$
- Run $q_0\, q_1 \ldots$ is accepting if for all $F \in \mathcal{F}$: $q_i \in F$ for infinitely many i
- $\sigma \in \Sigma^\omega$ is *accepted* by $\mathcal{G}$ if there exists an accepting run for σ
- The accepted language of $\mathcal{G}$:

$$\mathcal{L}_\omega(\mathcal{G}) = \left\{ \sigma \in \Sigma^\omega \mid \text{ there exists an accepting run for } \sigma \text{ in } \mathcal{G} \right\}$$

REVIEW: 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 k accept sets) into an equivalent NBA:
  - make k copies of the automaton
  - 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, move to the $(i+1)$-st copy

From LTL to GNBA (idea)

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

- Assume φ only contains the operators $\wedge$, $\neg$, $\bigcirc$ and U
  - $\vee$, $\rightarrow$, $\Diamond$, $\Box$, W, and so on, are expressed in terms of these basic operators
- States are elementary sets of sub-formulas in φ
  - for $\sigma = A_0 A_1 A_2 \ldots \in Words(\varphi)$,
    expand $A_i \subseteq AP$ with sub-formulas of φ
  - ... to obtain the infinite word $\overline{\sigma} = B_0 B_1 B_2 \ldots$ such that

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

  - $\overline{\sigma}$ is intended to be a run in GNBA $\mathcal{G}_\varphi$ for σ
- Transitions are derived from
  the semantics of $\bigcirc$ and the expansion law for U
- Accept sets guarantee that: $\overline{\sigma}$ 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 $A_0 = \{ a \}$, $A_1 = \{ a, b \}$, $A_2 = \{ b \}, \ldots$ 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 in the automaton (not on words)
- Result:

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

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

$B \subseteq closure(\varphi)$ is elementary if:

1. B is logically consistent if for all $\varphi_1 \wedge \varphi_2, \psi \in closure(\varphi)$:
    - $\varphi_1 \wedge \varphi_2 \in B \Leftrightarrow \varphi_1 \in B$ and $\varphi_2 \in B$
    - $\psi \in B \Rightarrow \neg\psi \notin B$
    - true $\in closure(\varphi) \Rightarrow$ true $\in B$
2. B is locally consistent if for all $\varphi_1 \,\mathsf{U}\, \varphi_2 \in closure(\varphi)$:
    - $\varphi_2 \in B \Rightarrow \varphi_1 \,\mathsf{U}\, \varphi_2 \in B$
    - $\varphi_1 \,\mathsf{U}\, \varphi_2 \in B$ and $\varphi_2 \notin B \Rightarrow \varphi_1 \in B$
3. B is maximal, i.e., for all $\psi \in closure(\varphi)$:
    - $\psi \notin B \Rightarrow \neg\psi \in B$

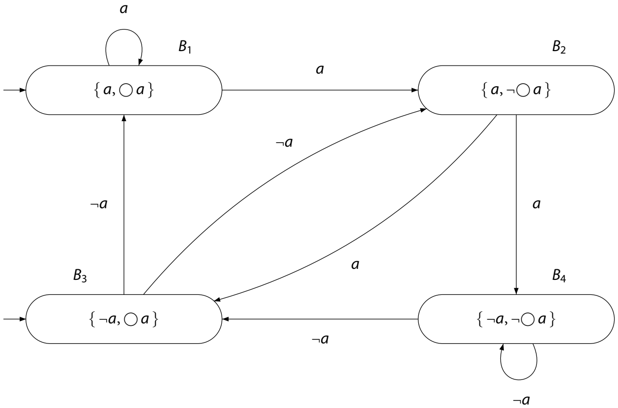
The GNBA of LTL-formula φ

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

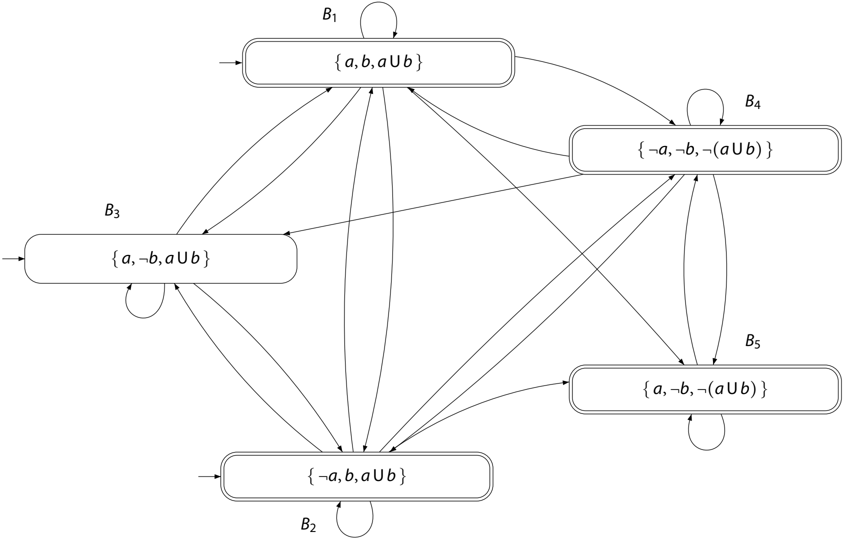
- Q is the set of all elementary sets of formulas $B \subseteq closure(\varphi)$
  - $Q_0 = \{ B \in Q \mid \varphi \in B \}$
- $\mathcal{F} = \{ \{ B \in Q \mid \varphi_1 \, \mathsf{U} \, \varphi_2 \notin B \text{ or } \varphi_2 \in B \} \mid \varphi_1 \, \mathsf{U} \, \varphi_2 \in closure(\varphi) \}$
- The transition relation $\delta : Q \times 2^{AP} \rightarrow 2^Q$ is given by:
  - $\delta(B, B \cap AP)$ is the set of all elementary sets of formulas B' satisfying:
    - (i) For every $\bigcirc \psi \in closure(\varphi)$: $\bigcirc \psi \in B \iff \psi \in B'$, and
    - (ii) For every $\psi_1 \, \mathsf{U} \, \psi_2 \in closure(\varphi)$:

$$\psi_1 \, \mathsf{U} \, \psi_2 \in B \iff \left(\psi_2 \in B \vee (\psi_1 \in B \wedge \psi_1 \, \mathsf{U} \, \psi_2 \in B') \right)$$

GNBA for LTL-formula $\bigcirc a$



GNBA for LTL-formula $a \cup b$



Main result

[Vardi, Wolper & Sistla 1986]

For any LTL-formula φ (over AP) there exists a GNBA $\mathcal{G}_\varphi$ over 2^{AP} such that:

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

(b) $\mathcal{G}_\varphi$ can be constructed in time and space $\mathcal{O}\left(2^{|\varphi|}\right)$

(c) #accepting sets of $\mathcal{G}_\varphi$ is bounded above by $\mathcal{O}(|\varphi|)$

$\Rightarrow$ every LTL-formula expresses an ω-regular property!

Proof

$Words(\varphi) \subseteq \mathcal{L}_\omega(\mathcal{G}_\varphi)$

- Let $\sigma = A_0 A_1 \ldots \in Words(\varphi)$.
- We construct an accepting run $B_0 B_1 \ldots$ of $\mathcal{G}_\varphi$ on σ as follows:
  $B_i = \{\psi \in closure(\varphi) \mid A_i A_{i+1} \ldots \models \psi\}$
  1. $B_0 B_1 \ldots$ is a run of $\mathcal{G}_\varphi$ on σ, because for all positions i:
     - $A_i = B_i \cap AP$
     - $\bigcirc \psi \in B_i$
       iff $A_i A_{i+1} A_{i+2} \ldots \models \bigcirc \psi$
       iff $A_{i+1} A_{i+2} \ldots \models \psi$
       iff $\psi \in B_{i+1}$
     - $\psi_1 \mathsf{U} \psi_2 \in B_i$
       iff $A_i A_{i+1} A_{i+2} \ldots \models \psi_1 \mathsf{U} \psi_2$
       iff $A_i A_{i+1} A_{i+2} \ldots \models \psi_2$ or $(A_i A_{i+1} \ldots \models \psi_1$ and $A_{i+1} A_{i+2} \ldots \models \psi_1 \mathsf{U} \psi_2)$
       iff $\psi_2 \in B_i$ or $(\psi_1 \in B_i$ and $\psi_1 \mathsf{U} \psi_2 \in B_{i+1})$

Proof (cont'd)

2. $B_0 B_1 \ldots$ is an accepting run, i.e., for every $\psi_{1,j} \, \mathsf{U} \, \psi_{2,j} \in \mathit{closure}(\varphi)$, $B_i \in F_j = \left\{ B \in Q \mid \psi_{1,j} \, \mathsf{U} \, \psi_{2,j} \notin B \text{ or } \psi_{j,2} \in B \right\}$ for infinitely many i.
    - Suppose $B_i \notin F_j$ for all $i \geq k$ for some k
    - $B_i \notin F_j \Rightarrow \psi_{1,j} \, \mathsf{U} \, \psi_{2,j} \in B_i$ and $\psi_{2,j} \notin B_i$
    - Hence, $A_i A_{i+1} \ldots \vDash \psi_{1,j} \, \mathsf{U} \, \psi_{2,j}$ and $A_i A_{i+1} \ldots \nvDash \psi_{2,j}$
    - Thus, $A_k A_{k+1} \ldots \vDash \psi_{1,j} \, \mathsf{U} \, \psi_{2,j}$ but $A_i A_{i+1} \ldots \nvDash \psi_{2,j}$ for all $i \geq k$.
    - Contradiction.

Proof (cont'd)

$\mathcal{L}_\omega(\mathcal{G}_\varphi) \subseteq Words(\varphi)$

- Let $A_0A_1 \ldots \in L_\omega(\mathcal{G}_\varphi)$ with accepting run $B_0B_1 \ldots$.
- We show that for all positions $i \geq 0$, $\psi \in B_i$ iff $A_iA_{i+1} \ldots \models \psi$.
  Proof by structural induction on ψ:
- $\psi \in AP$: Since $\delta(B, A) = \varnothing$ if $A \neq B \cap AP$, $A_i = B_i \cap AP$
- $\psi = \bigcirc \psi'$: By IH, $\psi' \in B_{i+1}$ iff $A_{i+1}A_{i+2} \ldots \psi'$.
  Hence, $\bigcirc \psi' \in B_i$ iff $A_iA_{i+1} \ldots \models \bigcirc \psi$
- $\psi = \psi_1 \wedge \psi_2$: By IH, ...
- $\psi = \neg\psi'$: By IH, ...
- $\psi = \psi_1 \,\mathsf{U}\, \psi_2$:
  1. $A_iA_{i+1} \ldots \models \psi \Rightarrow \psi \in B_i$:
     - Assume $A_iA_{i+1} \ldots \models \psi_1 \,\mathsf{U}\, \psi_2$.
     - There exists a $k \geq i$ s.t. $A_kA_{k+1} \ldots \models \psi_2$ and $A_jA_{j+1} \models \psi_1$ for all $i \leq j < k$
     - $\Rightarrow \psi_2 \in B_k$ and $\psi_1 \in B_j$ for all $i \leq j < k$
     - Hence, $\psi_1 \,\mathsf{U}\, \psi_2 \in B_k$, $\psi_1 \,\mathsf{U}\, \psi_2 \in B_{k-1}$, ..., $\psi_1 \,\mathsf{U}\, \psi_2 \in B_i$.

Proof (cont'd)

2. $\psi \in B_i \Rightarrow A_i A_{i+1} \ldots \models \psi$
   - Assume $\psi_1 \,\mathsf{U}\, \psi_2 \in B_i$
   - Case 1: $\psi_2 \notin B_j$ for all $j \geq i$:
     By ind. on j, $\psi_1 \in B_j$ and $\psi_1 \,\mathsf{U}\, \psi_2 \in B_j$ for all $j \geq i$
     $\Rightarrow B_j \notin \{ B \in Q \mid \psi_1 \,\mathsf{U}\, \psi_2 \notin B \text{ or } \psi_2 \in B \}$. Contradiction.
   - Case 2: There is a smallest $k \geq i$ with $\psi_2 \in B_k$.
     Hence, by IH, $A_k A_{k+1} \ldots \models \psi_2$
     By ind. on j, $i \leq j < k$, $\psi_1 \in B_j$, and
     hence, by IH, $A_j A_{j+1} \ldots \models \psi_1$
     $\Rightarrow A_i A_{i+1} A_{i+2} \ldots \models \psi_1 \,\mathsf{U}\, \psi_2$

NBA are more expressive than LTL

There is no LTL formula φ with $Words(\varphi) = P$ for the LT-property:

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

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!

Proof

- Proof by contradiction:
  Assume there is an LTL formula φ with $Words(\varphi) = P$.
- Let $w_1 = \{a\}^{n+1}\varnothing\{a\}^\omega$ and
  $w_2 = \{a\}^{n+2}\varnothing\{a\}^\omega$
  where n is the number of $\bigcirc$-operators in φ.
  We show that $w_1 \in Words(\varphi)$ iff $w_2 \in Words(\varphi)$.
  This contradicts $Words(\varphi) = P$.
  Structural induction on φ:
- $\varphi \in AP$: φ only depends on first position
- $\varphi = \bigcirc\psi$: by IH, $\{a\}^n\varnothing\{a\}^\omega \in Words(\psi)$ iff
  $\{a\}^{n+1}\varnothing\{a\}^\omega \in Words(\psi)$.
  Hence, $w_1 \in Words(\varphi)$ iff $w_2 \in Words(\varphi)$.

Proof (cont'd)

- $\varphi = \psi_1 \, \mathsf{U} \, \psi_2$:
  1. $w_1 \in Words(\varphi) \Rightarrow w_2 \in Words(\varphi)$:
     - Case 1: $w_1 \models \psi_2$. Then, by IH, $w_2 \models \psi_2$.
     - Case 2: $w_1 \not\models \psi_2$. Let k be the smallest index such that $w_1[k \ldots] \models \psi_2$ and $\forall 0 \leq i < k . w_1[i \ldots] \models \psi_1$.
       $\Rightarrow w_2[k+1, \ldots] \models \psi_2$ and $\forall 1 \leq i < k . w_2[i \ldots] \models \psi_1$.
       Additionally, by IH, $w_1 \models \psi_1 \Rightarrow w_2 \models \psi_1$.
  2. $w_2 \in Words(\varphi) \Rightarrow w_1 \in Words(\varphi)$
     - Case 1: $w_2 \models \psi_2$. Then, by IH, $w_1 \models \psi_2$.
     - Case 2: $w_2 \not\models \psi_2$. Let k be the smallest index such that $w_2[k \ldots] \models \psi_2$ and $\forall 0 \leq i < k . w_2[i \ldots] \models \psi_1$.
       $\Rightarrow w_1[k-1, \ldots] \models \psi_2$ and $\forall 1 \leq i < k-1 . w_1[i \ldots] \models \psi_1$.

Complexity for LTL to NBA

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

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 $2^{|\text{subf}(\varphi)|}$
  - where $\text{subf}(\varphi)$ denotes the set of all subformulae of φ
  - $|\text{subf}(\varphi)| \leq 2 \cdot |\varphi|$; 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 by $\mathcal{O}(|\varphi|)$
- The number of states in NBA $\mathcal{A}_\varphi$ is thus bounded by $2^{\mathcal{O}(|\varphi|)} \cdot \mathcal{O}(|\varphi|) = 2^{\mathcal{O}(|\varphi| + \log |\varphi|)} = 2^{\mathcal{O}(|\varphi|)}$ 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

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

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

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

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 (cont'd)

Claim: any NBA $\mathcal{A}$ for $\bigwedge_{a \in AP} \bigwedge_{0 \leq i < n} (\bigcirc^i a \longleftrightarrow \bigcirc^{n+i} a)$ 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 $q(A_1 \ldots A_n)$, 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 $\geq \left(|2^{AP}|\right)^n \geq 2^n$ states

Complexity for LTL model checking

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

On-the-fly LTL model checking

- Idea: find a counter-example during the generation of $Reach(TS)$ and $\mathcal{A}_{\neg\varphi}$
  - exploit the fact that $Reach(TS)$ and $\mathcal{A}_{\neg\varphi}$ can be generated in parallel

$\Rightarrow$ Generate $Reach(TS \otimes \mathcal{A}_{\neg\varphi})$ “on demand”

  - consider a new vertex only if no accepting cycle has been found yet
  - only consider the successors of a state in $\mathcal{A}_{\neg\varphi}$ that match current state in *TS*

$\Rightarrow$ Possible to find an accepting cycle without generating $\mathcal{A}_{\neg\varphi}$ entirely

- This on-the-fly scheme is adopted for example in the model checker SPIN

The LTL model-checking problem is co-NP-hard

The Hamiltonian path problem is polynomially reducible to the complement of the LTL model-checking problem

In fact, the LTL model-checking problem is PSPACE-complete

[Sistla & Clarke 1985]