Verification – Lecture 10
From LTL to NBA

Bernd Finkbeiner – Sven Schewe
Rayna Dimitrova – Lars Kuhtz – Anne Proetzsch

Wintersemester 2007/2008

REVIEW

Büchi automata

A *nondeterministic Büchi automaton* (NBA) $\mathcal{A}$ is a tuple $(Q, \Sigma, \delta, Q_0, F)$ 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
- $F \subseteq Q$ is a set of accept (or: final) states

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

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

Facts about Büchi automata

- They are as expressive as ω-regular languages
- Nondeterministic BA are more expressive than deterministic BA
- Emptiness check = check for reachable recurrent accept state
  - this can be done in $\mathcal{O}(|\mathcal{A}|)$

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

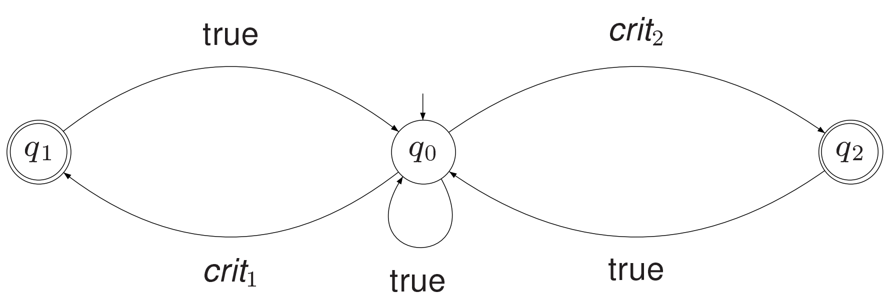
The size of $\mathcal{G}$, denoted $|\mathcal{G}|$, is the number of states and transitions in $\mathcal{G}$:

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

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 $0 \leqslant i$
- 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 $\mathcal{G}$:
  - $\mathcal{L}_\omega(\mathcal{G}) = \left\{ \sigma \in \Sigma^\omega \mid \text{ there exists an accepting run for } \sigma \text{ in } \mathcal{G} \right\}$
- GNBA $\mathcal{G}$ and $\mathcal{G}'$ are *equivalent* if $\mathcal{L}_\omega(\mathcal{G}) = \mathcal{L}_\omega(\mathcal{G}')$

Example



$\mathcal{F} = \{F_1, F_2\}; F_1 = \{q_1\}; F_2 = \{q_2\}$

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

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 $|\mathcal{A}| = \mathcal{O}(|\mathcal{G}| \cdot |\mathcal{F}|)$

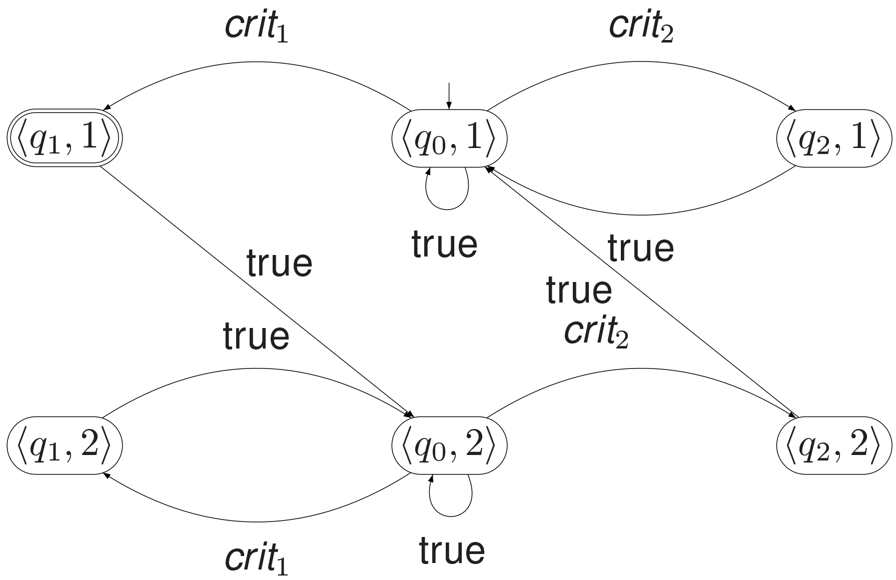
where $\mathcal{F}$ denotes the set of acceptance sets in $\mathcal{G}$

Construction

- Let $\mathcal{G} = (Q, \Sigma, \delta, Q_0, \mathcal{F})$ be the GNBA.
- We assume w.l.o.g that $\mathcal{F} = \{F_1, \ldots, F_k\}$ for $k \geqslant 1$. (otherwise just add Q to $\mathcal{F}$.)
- We construct the NBA $\mathcal{A} = (Q', \Sigma, \delta', Q'_0, F')$ where
  - $Q' = Q \times \{1, \ldots k\}$;
  - $Q'_0 = Q_0 \times \{1\}$;
  - $\delta(\langle q, i\rangle, A) = \begin{cases} \{\langle q', i\rangle \mid q' \in \delta(q, A)\} & \text{if } q \notin F_i, \\ \{\langle q', i+1\rangle \mid q' \in \delta(q, A)\} & \text{if } q \in F_i, i < k, \\ \{\langle q', 1\rangle \mid q' \in \delta(q, A)\} & \text{if } q \in F_i, i = k; \end{cases}$
  - $F' = F_1 \times \{1\}$.

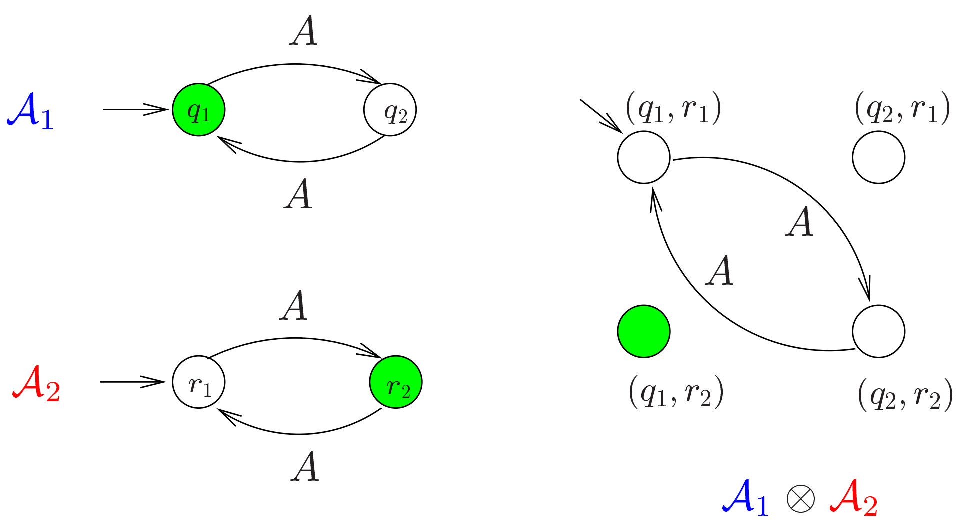
■

Example



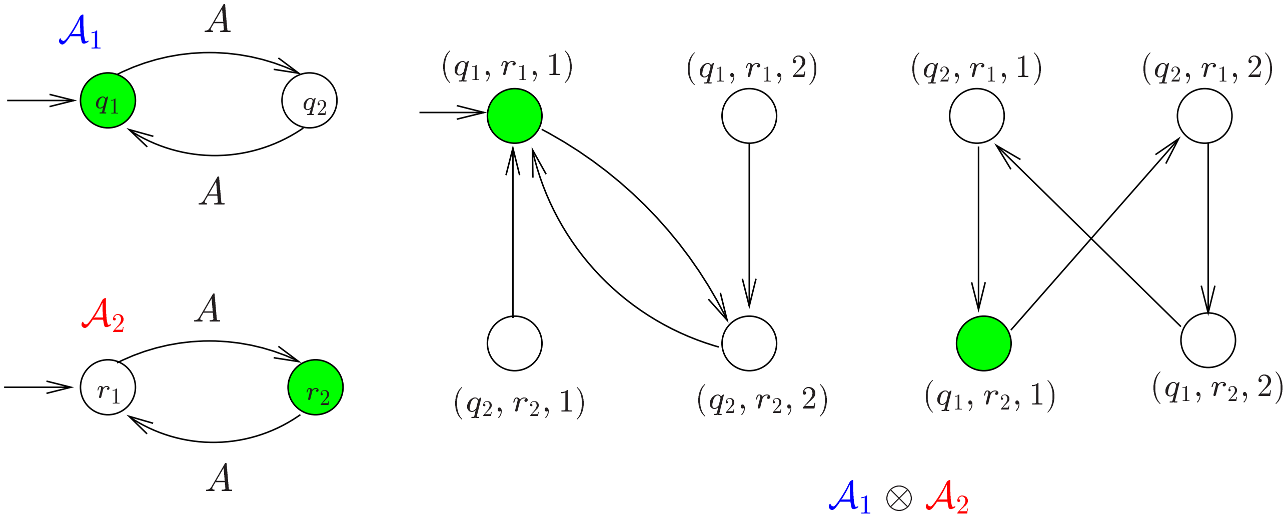
Product of Büchi automata

The product construction for finite automata does *not* work:



$\mathcal{L}_\omega(\mathcal{A}_1) = \mathcal{L}_\omega(\mathcal{A}_2) = \{ A^\omega \}$, but $\mathcal{L}_\omega(\mathcal{A}_1 \otimes \mathcal{A}_2) = \varnothing$

Product of Büchi automata



Intersection

For GNBA $\mathcal{G}_1$ and $\mathcal{G}_2$ there exists a GNBA $\mathcal{G}$ with
$\mathcal{L}_\omega(\mathcal{G}) = \mathcal{L}_\omega(\mathcal{G}_1) \cap \mathcal{L}_\omega(\mathcal{G}_2)$ and $|\mathcal{G}| = \mathcal{O}(|\mathcal{G}_1| \cdot |\mathcal{G}_2|)$

Construction

- Let $\mathcal{G}_1 = (Q_1, \Sigma, \delta_1, Q_{0,1}, \mathcal{F}_1)$ and $\mathcal{G}_2 = (Q_2, \Sigma, \delta_2, Q_{0,2}, \mathcal{F}_2)$.
- Construct $\mathcal{G} = (Q, \Sigma, \delta, Q_0, \mathcal{F})$ where
  - $Q = Q_1 \times Q_2$;
  - $Q_0 = Q_{0,1} \times Q_{0,2}$;
  - $\langle q_1', q_2' \rangle \in \delta(\langle q_1, q_2 \rangle, A)$ iff $q_1' \in \delta_1(q_1, A)$ and $q_2' \in \delta_2(a_2, A)$;
  - $\mathcal{F} = \{F_1 \times Q_2 \mid F_1 \in \mathcal{F}_1\} \cup \{Q_1 \times F_2 \mid F_2 \in \mathcal{F}_2\}$.

■

From LTL to NBA

Propositional linear-time temporal logic

Propositional LTL: assertion language = propositional logic

BNF grammar for LTL formulas over propositions *AP* with $a \in AP$:

$$\varphi ::= \text{true} \;\Big|\; a \;\Big|\; \varphi_1 \wedge \varphi_2 \;\Big|\; \varphi_1 \vee \varphi_2 \;\Big|\; \neg\varphi \;\Big|\; \bigcirc\varphi \;\Big|\; \Box\varphi \;\Big|\; \Diamond\varphi \;\Big|\; \varphi_1 \,\mathcal{W}\, \varphi_2 \;\Big|\; \varphi_1 \,\mathcal{U}\, \varphi_2$$

REVIEW

Expansion laws

$$\begin{aligned}
\Diamond\varphi &\equiv \varphi \vee \bigcirc\Diamond\varphi \\
\Box\varphi &\equiv \varphi \wedge \bigcirc\Box\varphi \\
\varphi\,\mathcal{U}\,\psi &\equiv \psi \vee (\varphi \wedge \bigcirc(\varphi\,\mathcal{U}\,\psi))
\end{aligned}$$

Sublogic

For the purposes of the construction, we can assume that our formulas only contain the operators $\wedge$, $\neg$, $\bigcirc$, and $\mathcal{U}$:

$$\begin{aligned} \varphi \vee \psi &\equiv \neg(\neg\varphi \wedge \neg\psi) \\ \Diamond \varphi &\equiv \text{true}\ \mathcal{U}\ \varphi \\ \Box \varphi &\equiv \neg(\Diamond \neg\varphi) \\ \varphi\ \mathcal{W}\ \psi &\equiv \varphi\ \mathcal{U}\ \psi \vee \Box \phi \end{aligned}$$

From LTL to GNBA: Idea

- States are *sets* of formulas:
  - for $\sigma = A_0 A_1 A_2 \ldots$, expand $A_i \subseteq AP$ with sub-formulas of φ
  - ... to obtain the infinite word $\bar{\sigma} = B_0 B_1 B_2 \ldots$ such that

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

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

From LTL to GNBA: Idea (cont'd)

- Example: $\varphi = a\,\mathcal{U}\,(\neg a \wedge b)$ 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

- 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 subformulas ψ of φ and their negation $\neg\psi$

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

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

Can we choose any subset of *closure*(φ) for B_i?

Elementary sets of formulae

$B \subseteq$ *closure*(φ) is *elementary* if:

1. B is *logically consistent* if for all $\varphi_1 \wedge \varphi_2, \psi \in$ *closure*(φ):
   - $\varphi_1 \wedge \varphi_2 \in B \;\Leftrightarrow\; \varphi_1 \in B$ 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 $\varphi_1 \mathcal{U} \varphi_2 \in$ *closure*(φ):
   - $\varphi_2 \in B \;\Rightarrow\; \varphi_1 \mathcal{U} \varphi_2 \in B$
   - $\varphi_1 \mathcal{U} \varphi_2 \in B$ and $\varphi_2 \notin B \;\Rightarrow\; \varphi_1 \in B$
3. B is *maximal*, i.e., for all $\psi \in$ *closure*(φ):
   - $\psi \notin B \;\Rightarrow\; \neg\psi \in B$

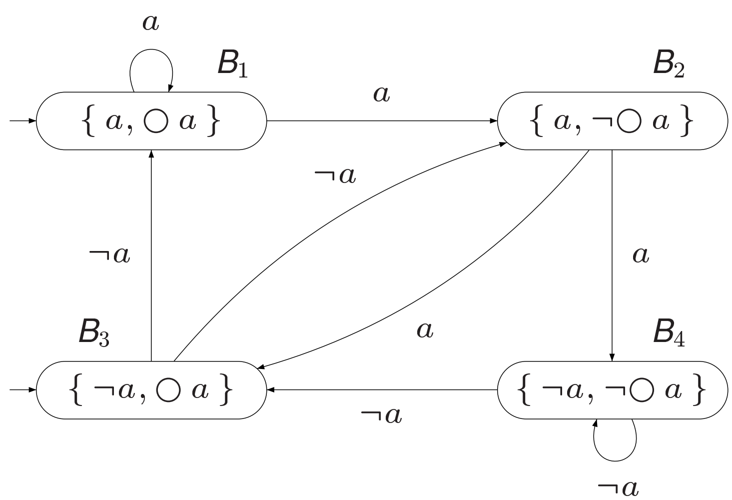
The GNBA of LTL-formula φ

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

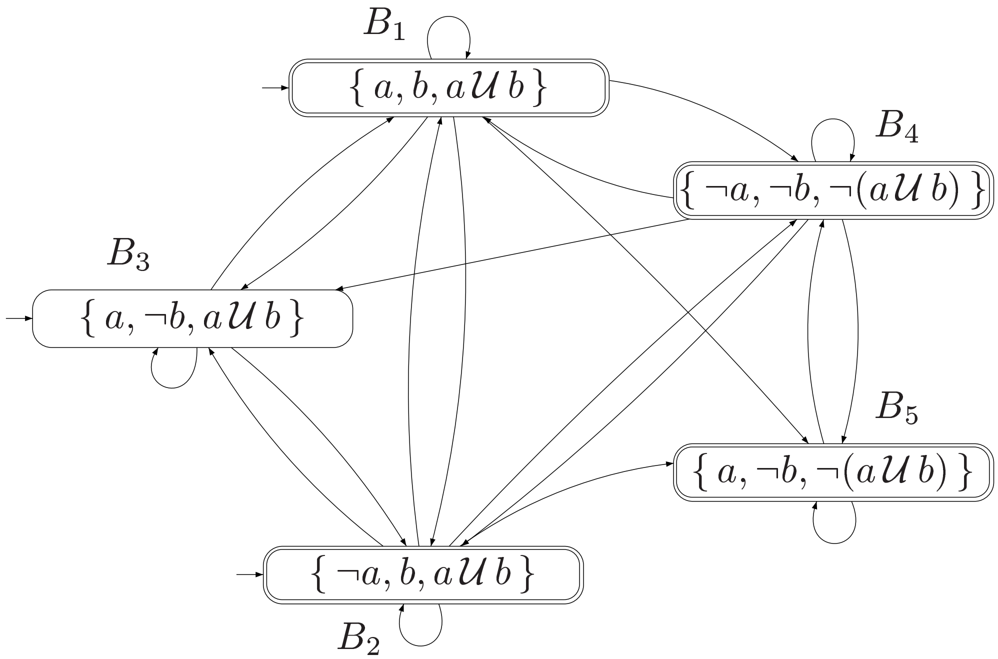
- Q is the set of all elementary sets of formulas $B \subseteq$ *closure*(φ)
  - $Q_0 = \left\{ B \in Q \mid \varphi \in B \right\}$
- $\mathcal{F} = \left\{ \left\{ B \in Q \mid \varphi_1 \mathcal{U} \varphi_2 \notin B \text{ or } \varphi_2 \in B \right\} \mid \varphi_1 \mathcal{U} \varphi_2 \in \textit{closure}(\varphi) \right\}$
- 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*(φ): $\bigcirc \psi \in B \;\Leftrightarrow\; \psi \in B'$, and
    (ii) For every $\varphi_1 \mathcal{U} \varphi_2 \in$ *closure*(φ):

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

GNBA for LTL-formula $\bigcirc a$



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



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) $\sigma \in \mathcal{L}_\omega(\mathcal{G}_\varphi)$ iff $\sigma \models \varphi$

(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!*