Verification – Lecture 9
Büchi Automata

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
- $\delta : Q \times \Sigma \to 2^Q$ 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 $\mathcal{A}$:

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

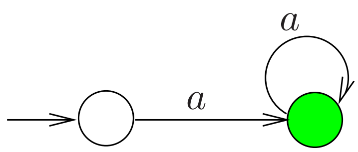
Language of an NBA

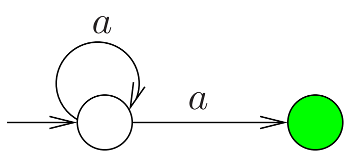
- NBA $\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$ and word $\sigma = A_0 A_1 A_2 \ldots \in \Sigma^\omega$
- A *run* for σ in $\mathcal{A}$ is an infinite sequence $q_0\, q_1\, q_2 \ldots$ such that:
  - $q_0 \in Q_0$ and $q_i \xrightarrow{A_i} q_{i+1}$ for all $0 \leqslant i$
- Run $q_0\, q_1\, q_2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

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

- NBA $\mathcal{A}$ and $\mathcal{A}'$ are *equivalent* if $\mathcal{L}_\omega(\mathcal{A}) = \mathcal{L}_\omega(\mathcal{A}')$

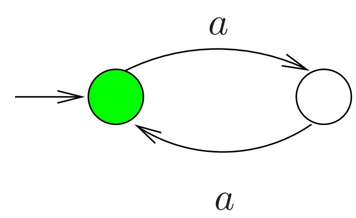
NBA versus NFA

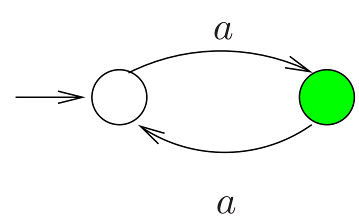




finite equivalence $\not\Rightarrow$ ω-equivalence

$\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{A}')$, but $\mathcal{L}_\omega(\mathcal{A}) \neq \mathcal{L}_\omega(\mathcal{A}')$





ω-equivalence $\not\Rightarrow$ finite equivalence

$\mathcal{L}_\omega(\mathcal{A}) = \mathcal{L}_\omega(\mathcal{A}')$, but $\mathcal{L}(\mathcal{A}) \neq \mathcal{L}(\mathcal{A}')$

NBA and ω-regular languages

- An ω*-regular expression* over the alphabet Σ has the form

$$G = E_1 \cdot F^{\omega} + \ldots + E_n \cdot F_n^{\omega}$$

where $n \geqslant 1$ and $E_1, \ldots, E_n, F_1, \ldots, F_n$ are regular expressions over Σ such that ϵ is not in the language of F_i for all $1 \leqslant i \leqslant b$.

- A language $\mathcal{L} \subseteq \Sigma^{\omega}$ is called ω-regular, if it is the language of some ω-regular expression.

- The class of languages accepted by NBA agrees with the class of ω-regular languages.

  Proof on the following slides.

Union of NBA

For NBA $\mathcal{A}_1$ and $\mathcal{A}_2$ (both over the alphabet Σ)

there exists an NBA $\mathcal{A}$ such that:

$\mathcal{L}_\omega(\mathcal{A}) = \mathcal{L}_\omega(\mathcal{A}_1) \cup \mathcal{L}_\omega(\mathcal{A}_2)$ and $|\mathcal{A}| = \mathcal{O}(|\mathcal{A}_1| + |\mathcal{A}_2|)$

Proof

- Let $\mathcal{A}_1 = (Q_1, \Sigma, \delta_1, Q_{0,1}, F_1)$ and $\mathcal{A}_2 = (Q_2, \Sigma, \delta_2, Q_{0,2}, F_2)$ be NBA over the same alphabet Σ.
- Assume w.l.o.g. that $Q_1 \cap Q_2 = \varnothing$.
- We construct $\mathcal{A}_1 + \mathcal{A}_2 = (Q_1 \cup Q_2, \Sigma, \delta, Q_{0,1} \cup Q_{0,2}, F_1 \cup F_2)$ where $\delta(q, A) = \begin{cases} \delta_1(q, A) & \text{if } q \in Q_1, \\ \delta_2(q, A) & \text{if } q \in Q_2. \end{cases}$
- Any accepting run in $\mathcal{A}_1$ or in $\mathcal{A}_2$ is an accepting run in $\mathcal{A}_1 + \mathcal{A}_2$.
- Any accepting run in $\mathcal{A}_1 + \mathcal{A}_2$ is either an accepting run in $\mathcal{A}_1$ or an accepting run in $\mathcal{A}_2$.

■

ω-operator for NFA

For each NFA $\mathcal{A}$ with $\varepsilon \notin \mathcal{L}(\mathcal{A})$ there exists an NBA $\mathcal{A}'$ such that:

$$\mathcal{L}_\omega(\mathcal{A}') = \mathcal{L}(\mathcal{A})^\omega \quad \text{and} \quad |\mathcal{A}'| = \mathcal{O}(|\mathcal{A}|)$$

Proof

- Let $\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$ be an NFA with $\epsilon \notin \mathcal{L}(\mathcal{A})$.

- **Step 1:** Ensure that all initial states have no incoming transitions and are not accepting.
  If $\mathcal{A}$ does not have this property, modify $\mathcal{A}$ as follows:

  – Add a new initial non-accept state q_{new} with transitions
  – $q_{\text{new}} \xrightarrow{\text{A}} q$ iff $q_0 \xrightarrow{\text{A}} q$ for some $q_0 \in Q_0$.
  – Set Q_0 to $\{q_{\text{new}}\}$.
  – This modification does not affect the language of $\mathcal{A}$.

- In the following, we assume that all initial states have no incoming transitions and that $Q_0 \cap F = \varnothing$.

Proof (cont'd)

- **Step 2:** Construct $\mathcal{A}' = (Q, \Sigma, \delta', Q_0, F')$:

  – $\delta'(q, A) = \begin{cases} \delta(q, A) & \text{if } \delta(q, A) \cap F = \varnothing, \\ \delta(q, A) \cup Q_0 & \text{otherwise;} \end{cases}$
  – $F' = Q_0$

- In the following, we show that $\mathcal{L}_\omega(\mathcal{A}') = \mathcal{L}(\mathcal{A})^\omega$.

Proof (cont'd): $\mathcal{L}_\omega(\mathcal{A}') = \mathcal{L}(\mathcal{A})^\omega$

$\subseteq$:
- Assume $\sigma \in \mathcal{L}_\omega(\mathcal{A}')$ and $q_0 q_1 q_2 \ldots$ is an accepting run for σ in $\mathcal{A}'$.
- Hence, $q_i \in F' = Q_0$ for infinitely many indices i: $i_0, i_1, i_2, \ldots$.
- Divide σ in subwords $\sigma = w_1 w_2 w_3 \ldots$ such that $q_{i_k} \in \delta'^*(q_{i_{k-1}}, w_k)$ for all $k \geqslant 1$.
- Since the states $q_{i_k} \in Q_0$ do not have any predecessors in $\mathcal{A}$, we get $\delta^*(q_{i_{k-1}}, w_k) \cap F \neq \varnothing$.
- This yields $w_k \in \mathcal{L}(\mathcal{A})$ for every $k \geqslant 1$.
- Hence, $\sigma \in \mathcal{L}(\mathcal{A})^\omega$.

Proof (cont'd): $\mathcal{L}_\omega(\mathcal{A}') = \mathcal{L}(\mathcal{A})^\omega$

$\supseteq$:
- Let $\sigma = w_1 w_2 w_3 \in \Sigma^\omega$ such that $w_k \in \mathcal{L}(\mathcal{A})$ for all $k \geqslant 1$.
- For each k, we choose an accepting run $q_0^k q_1^k q_2^k \ldots q_{n_k}^k$ of $\mathcal{A}$ on w_k.
- Hence, $q_0^k \in Q_0$ and $q_{n_k}^k \in F$ for all $k \geqslant 1$.
- Thus,
$$q_0^1 \ldots q_{n_1-1}^1 q_0^2 \ldots q_{n_2-1}^2 q_0^3 \ldots q_{n_3-1}^3 \ldots$$
is an accepting run for σ in $\mathcal{A}'$.
- Hence, $\sigma \in \mathcal{L}_\omega(\mathcal{A}')$.

■

Concatenation of an NFA and an NBA

For NFA $\mathcal{A}$ and NBA $\mathcal{A}'$ (both over the alphabet Σ)
there exists an NBA $\mathcal{A}''$ with
$\mathcal{L}_\omega(\mathcal{A}'') = \mathcal{L}(\mathcal{A}).\mathcal{L}_\omega(\mathcal{A}')$ and $|\mathcal{A}''| = \mathcal{O}(|\mathcal{A}| + |\mathcal{A}'|)$

Construction

- Let $\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$ be the NFA
  and $\mathcal{A}' = (Q', \Sigma, \delta', Q'_0, F')$ be the NBA with $Q \cap Q' = \varnothing$.
- Construct NBA $\mathcal{A}'' = (Q'', \Sigma, \delta'', Q''_0, F'')$:
  - $Q_0 = \begin{cases} Q_0 & \text{if } Q_0 \cap F = \varnothing, \\ Q_0 \cup Q'_0 & \text{otherwise;} \end{cases}$
  - $\delta''(q, A) = \begin{cases} \delta(q, A) & \text{if } q \in Q \text{ and } \delta(q, A) \cap F = \varnothing, \\ \delta(q, A) \cup Q'_0 & \text{if } q \in Q \text{ and } \delta(q, A) \cap F \neq \varnothing, \\ \delta'(q, A) & \text{if } q \in Q' \end{cases}$

■

NBA accept ω-regular languages

For each NBA $\mathcal{A}$: $\mathcal{L}_\omega(\mathcal{A})$ is ω-regular

Proof

- Define $\mathcal{L}_{qq'} = \{w \in \Sigma^* \mid q' \in \delta^*(q, w)\}$.
- Consider a word $\sigma \in \mathcal{L}(\mathcal{A})$ and an accepting run $q_0 q_1 q_2 \ldots$ for σ in $\mathcal{A}$.
- Hence, $q_i = q \in F$ for infinitely many indices i: $i_0, i_1, i_2, \ldots$.
- Divide σ in subwords $\sigma = w_1 w_2 w_3 \ldots$ such that

$$\sigma = \underbrace{w_0}_{\in \mathcal{L}_{q_0 q}} \underbrace{w_1}_{\in \mathcal{L}_{qq}} \underbrace{w_2}_{\in \mathcal{L}_{qq}} \underbrace{w_3}_{\in \mathcal{L}_{qq}} \ldots$$

- Hence,

$$\sigma \in \bigcup_{q_0 \in Q_0, q \in F} \mathcal{L}_{q_0 q}.(\mathcal{L}_{qq} \setminus \{\epsilon\})^\omega,$$

  which is ω-regular.

Proof (cont'd)

- On the other hand, any word

$$\sigma = \underbrace{w_0}_{\in \mathcal{L}_{q_0 q}} \underbrace{w_1}_{\in \mathcal{L}_{qq}} \underbrace{w_2}_{\in \mathcal{L}_{qq}} \underbrace{w_3}_{\in \mathcal{L}_{qq}} \ldots$$

  has an accepting run in $\mathcal{A}$.

- Hence, $\mathcal{L}_\omega(\mathcal{A})$ agrees with the ω-regular language

$$\sigma \in \bigcup_{q_0 \in Q_0, q \in F} \mathcal{L}_{q_0 q}.(\mathcal{L}_{qq} \setminus \{\epsilon\})^\omega.$$

■

Checking non-emptiness

$\mathcal{L}_\omega(\mathcal{A}) \neq \varnothing$ if and only if

$$\underbrace{\exists q_0 \in Q_0.\ \exists q \in F.\ \exists \mathsf{w} \in \Sigma^*.\ \exists \mathsf{v} \in \Sigma^+.\ \ q \in \delta^*(q_0, \mathsf{w}) \ \wedge \ q \in \delta^*(q, \mathsf{v})}_{\text{there is a reachable accept state on a cycle}}$$

The emptiness problem for NBA $\mathcal{A}$ can be solved in time $\mathcal{O}(|\mathcal{A}|)$

Non-blocking NBA

- NBA $\mathcal{A}$ is *non-blocking* if $\delta(q, A) \neq \varnothing$ for all q and $A \in \Sigma$
  - for each input word there exists an infinite run
- For each NBA $\mathcal{A}$ there exists a non-blocking NBA *trap*$(\mathcal{A})$ with:
  - $|\textit{trap}(\mathcal{A})| = \mathcal{O}(|\mathcal{A}|)$ and $\mathcal{A} \equiv \textit{trap}(\mathcal{A})$
- For $\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$ let *trap*$(\mathcal{A}) = (Q', \Sigma, \delta', Q_0, F)$ with:
  - $Q' = Q \cup \{ q_{trap} \}$ where $\{ q_{trap} \} \notin Q$
  -
$$\delta'(q, A) = \begin{cases} \delta(q, A) & : \text{ if } q \in Q \text{ and } \delta(q, A) \neq \varnothing \\ \{q_{trap}\} & : \text{ otherwise} \end{cases}$$

Deterministic BA

Büchi automaton $\mathcal{A}$ is called *deterministic* if

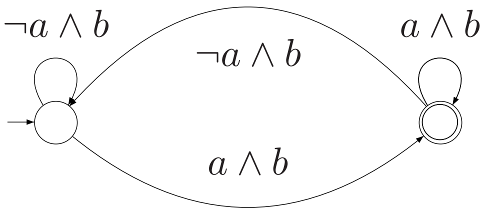
$$|Q_0| \leqslant 1 \quad \text{and} \quad |\delta(q, A)| \leqslant 1 \quad \text{for all } q \in Q \text{ and } A \in \Sigma$$

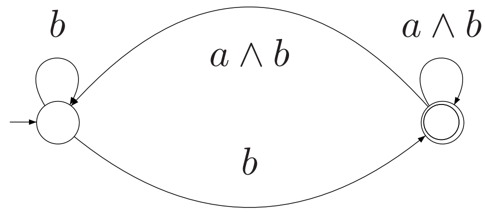
DBA $\mathcal{A}$ is called *total* if

$$|Q_0| = 1 \quad \text{and} \quad |\delta(q, A)| = 1 \quad \text{for all } q \in Q \text{ and } A \in \Sigma$$

total DBA provide unique runs for each input word

Example DBA for LT property





These NBA both represent the LT property "always b and infinitely often a"

NBA are more expressive than DBA

NFA and DFA are equally expressive but NBA and DBA are not!

There is no DBA that accepts $\mathcal{L}_\omega((A+B)^*B^\omega)$

Proof

- Proof by contradiction. Assume that $\mathcal{L} = \mathcal{L}_\omega((\mathsf{A}+\mathsf{B})^*\mathsf{B}^\omega) = \mathcal{L}_\omega(\mathcal{A})$ for some DBA $\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$.
- Since $\mathcal{A}$ is deterministic, we consider δ^* a function $Q \times \Sigma^* \to Q$.
- Since $B^\omega \in \mathcal{L}$, there exists an $n_1 \in \mathbb{N}_{\geqslant 1}$, such that

$$q_1 := \delta^*(q_0, B^{n_1}) \in F.$$

- Since $B^{n_1}AB^\omega \in \mathcal{L}$, there exists an $n_2 \in \mathbb{N}_{\geqslant 1}$, such that

$$q_2 := \delta^*(q_0, B^{n_1}AB^{n_2}) \in F.$$

Proof (cont'd)

- Continuing this process, we obtain an infinite sequence of numbers n_i and states q_i such that

$$q_i := \delta^*(q_0, B^{n_1}AB^{n_2}A \ldots B^{n_{i-1}}AB^{n_i}) \in F.$$

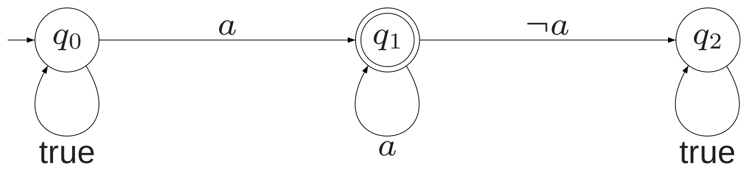
- Since $\mathcal{A}$ has only finitely many states, there exist i, j, such that $i < j$ and $q_i = q_j$.
- Thus, $\mathcal{A}$ has an accepting run on

$$w := B^{n_1}AB^{n_2}A \ldots AB^{n_i}(AB^{n_{i+1}}A \ldots AB^{n_j})^\omega.$$

- However, $w \notin \mathcal{L}$. Contradiction.

■

The need for nondeterminism



let $\{ a \} = AP$, i.e., $2^{AP} = \{A, B\}$ where $A = \{\}$ and $B = \{a\}$

"eventually forever a" equals $(A + B)^* B^\omega = (\{\} + \{a\})^* \{a\}^\omega$

Generalized Büchi automata

- NBA are as expressive as ω-regular languages
- Variants of NBA exist that are equally expressive
  - Muller, Rabin, and Streett automata
  - *generalized 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 $k{=}1$ this boils down to an NBA
- GNBA are useful to relate temporal logic and automata
  - but they are equally expressive as NBA

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

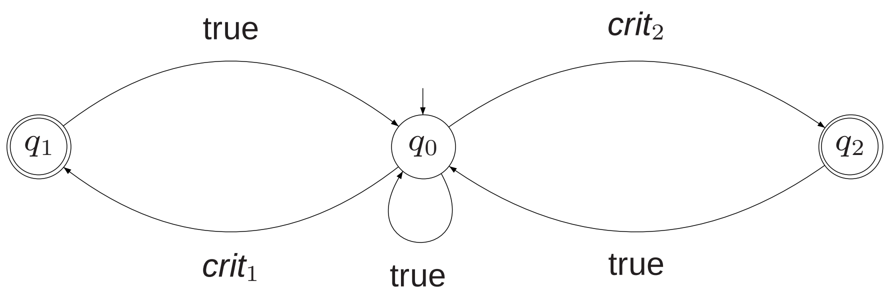
The size of $\mathcal{G}$, denoted $|\mathcal{G}|$, is the number of states and transitions in $\mathcal{G}$:

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

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 $\mathcal{G}$