Büchi Automata and Linear Temporal Logic

Joshua D. Guttman

Worcester Polytechnic Institute

18 February 2010
Büchi Automata

Definition

A Büchi automaton is a (non-deterministic) finite automaton.
Büchi Automata

Definition

A Büchi automaton is a (non-deterministic) finite automaton.

\[ \mathcal{A} = \langle Q, \Sigma, \delta, Q_s, F \rangle \]

where:

- \( Q \) is a finite set called the states
- \( \Sigma \) is a finite set called the alphabet
- \( \delta \subseteq Q \times \Sigma \times Q \), is called the transition relation
- \( Q_s \subseteq Q \) is called the set of initial states
- \( F \subseteq Q \) is called the set of accepting states
Büchi Automata: Runs, acceptance, language

Let $W$ be an infinite sequence $\langle w_0, w_1, \ldots \rangle$ with $w_i \in \Sigma$

- A *run $R$ of $A$ for $W$* is an infinite sequence $\langle r_0, r_1, \ldots \rangle$ with $r_i \in Q$ where
  1. $r_0 \in Q_s$
  2. $(r_i, w_i, r_{i+1}) \in \delta$

The language accepted by $A$, written $\text{lang}(A)$, is

$\{ W : A \text{ accepts } W \}$
Büchi Automata: Runs, acceptance, language

Let $W$ be an infinite sequence $\langle w_0, w_1, \ldots \rangle$ with $w_i \in \Sigma$

- A run $R$ of $A$ for $W$: an infinite sequence $\langle r_0, r_1, \ldots \rangle$ with $r_i \in Q$ where
  1. $r_0 \in Q_s$
  2. $(r_i, w_i, r_{i+1}) \in \delta$

- $A$ accepts $W$ iff there is some run $R$ for $W$ where:

$$\{ i : r_i \in F \} \text{ is infinite}$$
Büchi Automata: Runs, acceptance, language

Let $W$ be an infinite sequence $\langle w_0, w_1, \ldots \rangle$ with $w_i \in \Sigma$

- **A run $R$ of $A$ for $W$:** an infinite sequence $\langle r_0, r_1, \ldots \rangle$ with $r_i \in Q$
  - 1. $r_0 \in Q_s$
  - 2. $(r_i, w_i, r_{i+1}) \in \delta$

- **$A$ accepts $W$** iff there is some run $R$ for $W$ where:
  \[
  \{ i : r_i \in F \} \text{ is infinite}
  \]

- The **language accepted by $A$, written $\text{lang}(A)$**, is
  \[
  \{ W : A \text{ accepts } W \}\]
Some Büchi Automata, 1

$\Sigma = \{a, b\}$

$F = \{2\}$

Accepts $W$ iff $W$ has infinitely many $a$'s
Some Büchi Automata, 1

\[ \Sigma = \{a, b\} \]

\[ F = \{2\} \]

Accepts \( W \) iff \( W \) has infinitely many \( a \)s
Some Büchi Automata, 2

$\Sigma = \{a, b\}$

$F = \{2\}$

Accepts $W$ iff $W$ has finitely many $a$'s Can transition to state 2 after last $a$ received
Some Büchi Automata, 2

$\Sigma = \{a, b\}$

$F = \{2\}$

Accepts $W$ iff $W$ has finitely many $a$s

Can transition to state 2 after last $a$ received
There exists a $W \in \text{lang}(A)$ if there is a $q$ with a path from a start state to $q$ and a cycle $q \to + q$. $F = \{2\}$
Testing Non-Emptiness

There exists a $W \in \text{lang}(\mathcal{A})$ if there is a $q$ with

1. a path from a start state to $q$
2. a cycle $q \rightarrow^+ q$
Closure Conditions on Languages

Suppose given Büchi automata $A_1, A_2$

there exist Büchi automata with languages:

$$\text{lang}(A_1) \cup \text{lang}(A_2)$$

$$\text{lang}(A_1) \cap \text{lang}(A_2)$$

$$\Sigma^\omega \setminus \text{lang}(A_1)$$
Büchi Automata Representing LTL formula \( \varphi \nabla \)
\( \varphi \) contains atomic formulas \( \mathcal{L} \)

\[ \Sigma: \text{ Input letters are prop. logic models } \mathbb{M} \subseteq \mathcal{L} \]

\[ Q: \text{ Each subformula of } \varphi \text{ is a state, plus } \bot, \top, \ldots \]

\[ \delta(\psi, \mathbb{M}): \text{ depends on form of } \psi: \]

\[ \top, \text{ if } \psi \text{ in prop. logic and } \mathbb{M} \models \psi \]

\[ \bot, \text{ if } \psi \text{ in prop. logic and } \mathbb{M} \not\models \psi \]
Büchi Automata Representing LTL formula \( \varphi \)

\( \varphi \) contains atomic formulas \( \mathcal{L} \)

\[ \Sigma: \text{Input letters are prop. logic models } \mathcal{M} \subseteq \mathcal{L} \]

\[ Q: \text{Each subformula of } \varphi \text{ is a state, plus } \perp, \top, \ldots \]

\[ \delta(\psi, \mathcal{M}): \text{depends on form of } \psi: \]

- \( \top \), if \( \psi \) in prop. logic and \( \mathcal{M} \models \psi \)
- \( \perp \), if \( \psi \) in prop. logic and \( \mathcal{M} \not\models \psi \)
- \( \chi \), if \( \psi \) is \( X(\chi) \) and,
Büchi Automata Representing LTL formula $\varphi$

$\varphi$ contains atomic formulas $\mathcal{L}$

$\Sigma$: Input letters are prop. logic models $\mathbb{M} \subseteq \mathcal{L}$

$Q$: Each subformula of $\varphi$ is a state, plus $\bot, \top, \ldots$

$\delta(\varphi, \mathbb{M})$: depends on form of $\varphi$:

$\top$, if $\varphi$ in prop. logic and $\mathbb{M} \models \varphi$

$\bot$, if $\varphi$ in prop. logic and $\mathbb{M} \not\models \varphi$

$\chi$, if $\varphi$ is $X(\chi)$ and,

if $\varphi$ is $\alpha U \beta$,

$$\delta(\beta, \mathbb{M}) \lor (\delta(\alpha, \mathbb{M}) \land (\alpha U \beta))$$
Büchi Automata Representing LTL formula $\varphi$

$\varphi$ contains atomic formulas $L$

$\Sigma$: Input letters are prop. logic models $M \subseteq L$

$Q$: Each subformula of $\varphi$ is a state, plus $\bot, \top, \ldots$

$\delta(\psi, M)$: depends on form of $\psi$:

- $\top$, if $\psi$ in prop. logic and $M \models \psi$
- $\bot$, if $\psi$ in prop. logic and $M \not\models \psi$
- $\chi$, if $\psi$ is $X(\chi)$ and,

if $\psi$ is $\alpha U \beta$,

$$\delta(\beta, M) \lor (\delta(\alpha, M) \land (\alpha U \beta))$$

$F$: $\{\psi \in Q : \psi = \neg(\alpha U \beta)\}$
Suppose we are given:

- A Kripke structure $\mathcal{K}$
  - Represents a system
- An LTL formula $\varphi$
  - Represents a specification
  - “correctness condition”
Model Checking, 1: What?

Suppose we are given:

- A Kripke structure $\mathcal{K}$
  - Represents a system
- An LTL formula $\varphi$
  - Represents a specification
    - “correctness condition”

Does every execution of $\mathcal{K}$ satisfy $\varphi$?
Model Checking, 1: What?

Suppose we are given:

- A Kripke structure $\mathcal{K}$
  - Represents a system
- An LTL formula $\varphi$
  - Represents a specification
    - “correctness condition”

Does every execution of $\mathcal{K}$ satisfy $\varphi$?

For every $\pi$ over graph $\mathcal{K}$, does $\pi \models \varphi$ hold?
Model Checking, 2: How?

Let $\alpha$ be an LTL formula over atoms $\mathcal{L}$
Let $\mathcal{K} = (S, I, T, L)$ be a finite Kripke structure with $L(s) \subseteq \mathcal{L}$

- $\neg \alpha$ determines an automaton $A$

$\emptyset = \text{lang}(A) \cap \text{lang}(B)$
Let $\alpha$ be an LTL formula over atoms $\mathcal{L}$
Let $\mathcal{K} = (S, I, T, L)$ be a finite Kripke structure with $L(s) \subseteq \mathcal{L}$
- $\neg \alpha$ determines an automaton $A$
- $\mathcal{K}$ determines a Büchi automaton

$$B = S', \Sigma, \delta, I, S$$

where $S' = S \cup \{\text{fail}\}$  $\Sigma = 2^{\mathcal{L}}$, and

$$\delta(s, M) = \{s' \in T(s): L(s) = M\}$$

$$\cup \{\text{fail}: s = \text{fail or } L(s) \neq M\}$$
Let $\alpha$ be an LTL formula over atoms $\mathcal{L}$.

Let $\mathcal{K} = (S, I, T, L)$ be a finite Kripke structure with $L(s) \subseteq \mathcal{L}$.

- $\neg \alpha$ determines an automaton $A$.
- $\mathcal{K}$ determines a Büchi automaton $B$.

$$B = S', \Sigma, \delta, I, S$$

where $S' = S \cup \{\text{fail}\}$, $\Sigma = 2^\mathcal{L}$, and

$$\delta(s, M) = \{s' \in T(s): L(s) = M\}$$

$$\cup \{\text{fail}: s = \text{fail} \text{ or } L(s) \neq M\}$$

- $\emptyset \supseteq \text{lang}(A) \cap \text{lang}(B)$