Büchi Automata and LTL model checking

- Büchi Automata recognize infinite words.
- Can be used for LTL model checking:
  Given an LTL formula and a model:
  1. Build a Büchi Automaton F that accepts all executions that fail the LTL formula.
  2. Build a Büchi Automaton M that accepts all executions of the model.
  3. Build the product automaton $F \times M$ that accepts the intersection.
  4. Test for emptiness of $F \times M$.
     - If empty then the formula holds.
     - If non-empty then you have found a counter-example.

A Büchi Automaton over a signature Σ is a structure

$$(S, S^0, \rho, F)$$

where

- S is a finite set of states
- $S^0 \subseteq S$ is a set of initial states
- $\rho : S \times \Sigma \to 2^S$ is a transition function
- $F \subseteq S$ is a set of accepting states

- A run on an infinite word

$$a_1\, a_2 \cdots (a_i \in \Sigma)$$

  is a sequence

$$s_1\, s_2 \cdots (s \in S)$$

  such that

$$s_1 \in S^0 \qquad s_{i+1} \in \rho(s_i, a_i)$$

- A run is accepting if the set $\{i \mid s_i \in F\}$ is infinite.

- A Büchi Automaton (S, S^0, ρ, F) is deterministic if

$$\forall s \in S, a \in \Sigma : |\rho(s, a)| = 1$$

- Non-deterministic Büchi Automata are strictly more powerful than deterministic Büchi Automata

Proof

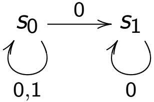
The language of all words with finitely many ones

$$L = \{(0|1)^* 0^\omega\}$$

can be recognized by a non-deterministic Büchi Automaton, but not by a deterministic one.

possible with non-determinism

The automaton



recognizes L (initial state s_0, accepting state s_1).

impossible without non-determinism

Suppose L can be recognized by a deterministic automaton with n states.
Then executing inputs 0^n from any reachable state, we must have passed through an accepting state. Otherwise we could not recognize 0^ω.
That means that executing $0^n 1$ from any reachable state, also passes through an accepting state. Hence the automaton accepts $(0^n 1)^\omega$.
Contradiction.

Construction for intersection

Given Büchi Automata $A_1 \equiv (S_1, S_1^0, \rho_1, F_1)$ and $A_2 \equiv (S_2, S_2^0, \rho_2, F_2)$.
Let $A \equiv (S, S^0, \rho, F)$ where

- $S = S_1 \times S_2 \times \{1, 2\}$
- $S^0 = S_1^0 \times S_2^0 \times \{1\}$
- $F = F_1 \times S_2 \times \{1\}$
- $\rho((s_1, s_2, i), a) = \{(t_1, t_2, k \mid \quad t_1 \in \rho_1(s_1, a), t_2 \in \rho_2(s_2, a)$
  $k = (s_i \in F_i)?(3 - i) : i\}$

Then A accepts iff both A_1 and A_2 accept.

Alternation

- For a set X, we define

$$\mathcal{B}^+(X) ::= x \mid \text{true} \mid \text{false} \mid \phi_1 \vee \phi_2 \mid \phi_1 \wedge \phi_2$$

  where $x \in X$, $\phi_i \in \mathcal{B}^+(X)$.
- An alternating (Büchi) automaton is a structure (S, s^0, ρ, F) where
  - S is a finite set of states
  - $s^0 \in S$ is an initial states
  - $\rho : S \times \Sigma \to \mathcal{B}^+(S)$ is a transition function
  - $F \subseteq S$ is a set of accepting states

- A run on a word $a_1, \cdots, a_n$ ($a_1, a_2, \cdots \; n = \infty$) is a (possibly infinite) tree, whose nodes are labeled with states, such that
  - The root is labeled with s^0.
  - Every node has at most $|S|$ children
  - If a node v at depth $k < n$ is labeled with the state s then the children $v_1, \cdots, v_r$ of v are labeled with states $s_1, \cdots, s_r$ such that

    $$s_1 \wedge \cdots \wedge s_r \rightarrow \rho(s, a_k)$$

    is valid.
- A run is accepting if all nodes at depth n are labeled with states from F.
- A run is Büchi accepting if every infinite branch contains infinitely many nodes with labels in F.

Alternating vs non-deterministic Büchi Automata

Let $NBA \equiv (S, S^0, \rho, F)$ be a non-deterministic Büchi Automaton.
Without loss of generality $S^0 = \{s^0\}$.
Define the alternating Büchi Automaton

$$ABA \equiv (S, s^0, (s,a) \mapsto \bigvee \rho(s,a), F)$$

Then NBA and ABA accept the same language.

Alternating vs non-deterministic Büchi Automata

Let $ABA \equiv (S, s^0, \rho, F)$ be an alternating Büchi Automaton
Define the non-deterministic Büchi automaton

$$NBA \equiv (2^S \times 2^S, \{(\{s^0\}, \emptyset)\}, \rho', \{\emptyset\} \times F)$$

where

$$\begin{aligned}
\rho'((U,V),a) = \quad & \{(X \setminus F, Y \cup (X \cap F)) \mid \exists X, Y \subset S \\
& \bigwedge X \to \bigwedge_{t \in U} \rho(t,a) \\
& \bigwedge Y \to \bigwedge_{t \in V} \rho(t,a)\} \\
\rho'((\emptyset,V)) = \quad & \{(Y \setminus F, Y \cap F) \mid \exists X, Y \subset S \\
& \bigwedge Y \to \bigwedge_{t \in V} \rho(t,a)\}
\end{aligned}$$

Then NBA and ABA accept the same language.