Automata and Grammars (BIE-AAG)

10. Properties of regular languages

Jan Holub

Department of Theoretical Computer Science
Faculty of Information Technology
Czech Technical University in Prague

Pumping lemma - problem statement

Let us assume that language $L = \{0^n 1^n : n >= 1\}$ is regular.

In such case language L is accepted by a finite automaton A with k states.

Pumping lemma - problem statement

Let the automaton A read a sequence O^k. While reading this sequence, the automaton must go through the following states:

ε	p_0
0	p_1
00	p_2
...	...
0^k	p_k

That is, $\exists i < j : p_i = p_j$ (pigeonhole principle). Let us denote such state by q.

Pumping lemma - problem resolution

Let us furthemore assume that reading an input sequence 1^i makes the automaton go from state q to state r.
It holds that:

- If state r is a final state, then the automaton accepts string $0^j 1^i$, which is unwanted.
- If state r is not a final state, then the automaton does not accept string $0^i 1^i$, which is unwanted as well.

By contradiction, language $L = \{0^n 1^n : n >= 1\}$ cannot be regular.

Pumping lemma formally

Let L be a regular language. Then for language L there exists a constant $p >= 1$ such that for every sentence $w \in L$ it holds that:
If $|w| \geq p$, then w has form $w = xyz$ such that:

- $y \neq \varepsilon$ (same as saying that $|y| \geq 1$),
- $|xy| \leq p$,
- $\forall i \geq 0$ it holds that sentence $xy^iz \in L$.

Pumping lemma formally

See the informal explanation above. For regular language L there exists a finite automaton that contains a loop. This loop reads a non-empty substring y. It holds that this loop can "pump"any number of times. If $xyz \in L$, then also for every i-fold "pumping"for $i \geq 0$ it holds that sentence $xy^iz \in L$.

Using PL for proving that L is not reg.

Proof that language $L = \{0^n1^n : n >= 1\}$ is not regular

Let us assume that L is regular. Then by pumping lemma it must hold that there is a constant $p \geq 1$ such that for every sentence $w \in L$ it holds that:

If $|w| \geq p$, then w has form $w = xyz$ such that:

- $y \neq \varepsilon$ (same as saying that $|y| \geq 1$),
- $|xy| \leq p$,
- $\forall i \geq 0$ it holds that sentence $xy^iz \in L$.

Let us assume a sentence $w = 0^p1^p \in L$ that is longer than p and therefore must meet the PL's requirements. To prove L is not regular, we now try all possible partitionings of w into xyz. We must prove that pumping lemma holds for none of them.

Using PL for proving that L is not reg.

Proof that language $L = \{0^n1^n : n >= 1\}$ is not regular

According to the two first conditions it must hold that:

- xy is a non-empty sequence of zeroes
- y is non-empty sequence of zeroes
- z contains all the ones.

But then xy^0z (that is, we remove y from $w = xyz$) does not belong to L (because the number of zeroes in xy^0z is surely less than the number of ones)!

Therefore pumping lemma does not hold for L and L is not regular.

Using PL for proving that L is not reg.

Proof that language $L = \{1^m : m$ is prime $\}$ is not regular

Let us assume that L is regular. Then by the pumping lemma it must hold that there exists a constant $p \geq 1$ such that ... (see Pumping lemma).

Let us assume sentence $w = 1^m$ for prime $m \geq p + 2$.

Now let us assume partitioning $w = xyz$ and a "pumped"sentence $w_1 = xy^{m-|y|}z$. We show that w_1 is not in L, which contradicts Pumping lemma.

Using PL for proving that L is not reg.

Proof that language $L = \{1^m : m$ is prime $\}$ is not regular

Let us consider the length of the sentence $w_1 = xy^{m-|y|}z$. It holds that
$|xy^{m-|y|}z| =$
$|xz| + (m - |y|) * |y| =$
$(m - |y|) + (m - |y|) * |y| =$
$(m - |y|) * (1 + |y|) =$.

w_1 would be a prime only if either $(m - |y|)$ or $(1 + |y|)$ were equal to 1.

Using PL for proving that L is not reg.

Proof that language $L = \{1^m : m$ is prime $\}$ is not regular

- $(1 + |y|) \neq 1$, because $|y| \geq 1$.
- $m >= p + 2$, $|y| \leq |xy| \leq p$, therefore $m - |y| \geq p + 2 - p = 2$.

Therefore, pumping lemma does not hold for L. For an arbitrary partitioning of $w = xyz \in L$ by the first two conditions of PL it holds that $xy^{m-|y|}z$ is not in L.

Therefore, L **is not regular**.

A question to check your comprehension

How big is the constant p in Pumping lemma for a *finite* regular language?

(Note: Every finite regular language is regular, therefore pumping lemma must hold for it.)

Myhill-Nerode theorem: motivation

- It characterizes fundamental relationships between finite automata over alphabet T and certain equivalence relations over strings in $T*$,
- it describes some of the necessary and sufficient conditions for a language to be regular (used often for proving that a language is not regular),
- it provides a formal basis for an elegant proof of existence of a unique (with respect to isomorphism) minimal DFA for a given regular language.

Right congruence and prefix equivalence

Definition
Equivalence $\sim$ is a binary relation that is *reflexive, symmetric* and *transitive*.

Definition
Equivalence class of an element a in set X is the subset of all elements in X that are equivalent to a.

Definition
The set of all equivalence classes in X is called the *quotient set* of X by $\sim$ and is denoted by $X/\sim$.

Definition
Index of equivalence $\sim$ is the number of equivalence classes in the quotient set $\Sigma/\sim$. If there are infinitely many equivalence classes, the index is defined to be ∞.

Right congruence and prefix equivalence

Definition
Let Σ be an alphabet and $\sim$ is an equivalence on Σ^*. Equivalence $\sim$ is a *right congruence*, if for every $u, v, w \in \Sigma^*$ it holds that:

$$u \sim v \Rightarrow uw \sim vw$$

Definition
Let L be an arbitrary (not necessarily regular) language over alphabet Σ. We define *prefix equivalence* for L, a relation $\sim_L$ on set Σ^* like this:

$$u \sim_L v \Leftrightarrow \forall w \in \Sigma^* : uw \in L \Leftrightarrow vw \in L$$

Myhill-Nerode theorem

Definition
Let L be a language over Σ. Then the following statements are equivalent:

1. L is a language accepted by a finite automaton.
2. L is a union of certain equivalence classes of the quotient set of Σ^* by the right congruence on Σ^* with a finite index.
3. Relation $\sim_L$ has a finite index.

Proof. We prove the following implications:

- $1 \Rightarrow 2$.
- $2 \Rightarrow 3$.
- $3 \Rightarrow 1$.

The theorem is then implied by propositional calculus.

Myhill-Nerode theorem: $1 \Rightarrow 2$

If L is accepted by a DFA, then L is a union of some classes of the quotient set by the right congruence on Σ^* with a finite index.

Let us introduce a general transition function $\hat{\delta}$ for DFA $M = (Q, \Sigma, \delta, q_0, F)$.
$\hat{\delta} : Q \times \Sigma^* \to Q$ such that
$\forall q_1, q_2 \in Q, w \in \Sigma^* : \hat{\delta}(q1, w) = q2 \Leftrightarrow (q1, w) \vdash_M^* (q2, \varepsilon)$.

Myhill-Nerode theorem: $1 \Rightarrow 2$

Proof. For a given L accepted by DFAM we construct $\sim$ with the necessary properties:

- Let $M = (Q, \Sigma, \delta, q_0, F)$ and δ is total.
- We set $\sim$ as a binary relation on Σ^* such that $u \sim v \Leftrightarrow \hat{\delta}(q_0, u) = \hat{\delta}(q_0, v)$.
- We show that $\sim$ has the necessary properties:
  - $\sim$ is an equivalence: it is reflexive, transitive and symmetric.
  - $\sim$ has a finite index: the equivalence classes correspond to the automaton states.
  - $\sim$ is a right congruence: Let $u \sim v$ and $a \in \Sigma$. Then $\hat{\delta}(q0, ua) = \delta(\hat{\delta}(q0, u), a) = \delta(\hat{\delta}(q0, v), a) = \hat{\delta}(q0, va)$ and therefore $ua \sim va$.
  - L is a union of some equivalence classes of $\Sigma^*/\sim$ – those that correspond to F.

Myhill-Nerode theorem: $2 \Rightarrow 3$

If there is a relation $\sim$ that satisfies condition 2, then $\sim_L$ has a finite index.

Proof.

- For all $u, v \in \Sigma$ such that $u \sim v$, it holds that $u \sim_L v$:
  - Let $u \sim v$. We will show that also $u \sim_L v$, that is $\forall w \in \Sigma^* : uw \in L \Leftrightarrow vw \in L$.
  - We know that $uw \sim vw$ and because L is a union of some classes of the quotioent set $\Sigma^*/\sim$, it also holds that $uw \in L \Leftrightarrow vw \in L$.
- We therefore know that $\sim \subseteq \sim_L$ (that is, $\sim_L$ is the largest right congruence with the given properties).
- Every class of $\sim$ is contained in some class of $\sim_L$.
- Index of $\sim_L$ cannot be greater than index of $\sim$.
- $\sim$ has a finite index and therefore even $\sim_L$ has a finite index.

Myhill-Nerode theorem: $3 \Rightarrow 1$

If $\sim_L$ has a finite index, then L is accepted by some finite automaton.

Proof.

- We create $M = (Q, \Sigma, \delta, q_0, F)$ accepting L:
  - $Q = \Sigma^*/\sim_L$ (states are the classes of the quotient set),
  - $\forall u \in \Sigma^*, a \in \Sigma : \delta([u], a) = [ua]$,
  - $q_0 = [\varepsilon]$,
  - $F = \{[x] | x \in L\}$.
- The shown construction is correct, that is $L = L(M)$:
- We show by induction over the length of word v that $\forall v \in \Sigma^* : \hat{\delta}([\varepsilon], v) = [v]$.
- $v \in L \Leftrightarrow [v] \in F \Leftrightarrow \hat{\delta}([\varepsilon], v) \in F$.

Proof of irregularity using M-N

Prove that language $L = \{0^n 1^n : n >= 1\}$ is not regular.

Proof.

- No strings $\varepsilon, 0, 0^2, 0^3, ...$ are $\sim_L$-equivalent, because $0^i 1^i \in L$, but $0^i 1^j \notin L$ for $i \neq j$.
- L therefore has infinitely many classes (or infinite index).
- According to Myhill-Nerode theorem L cannot be accepted by a finite automaton. □

M-N theorem and DFA minimality

Theorem (second version of M-N theorem)
Number of states of any minimal DFA accepting L is equal to index of $\sim_L$. (Such a DFA exists if and only if the index is finite.)

Proof.

- Every DFA (one can consider DFAs without unreachable states) defines a certain right congruence with a finite index and vice versa.
- If L is regular, $\sim_L$ is the greatest right congruence with a finite index such that L is the union of certain classes of the appropriate quotient set.
- Finite automaton that corresponds to $\sim_L$ (see proof of $3 \Rightarrow 1$ of M-N), is therefore a minimal DFA accepting L. □