Myhill-Nerode Theorem

Raju Hazari

Department of Computer Science and Engineering
National Institute of Technology Calicut

November 2, 2020

Myhill-Nerode Theorem

It state that following three statements are equivalent:

1. The language $L \subseteq \Sigma^*$ is accepted by some FSA.
2. L is the union of some of the equivalence classes of a right invariant equivalence relation of finite index.
3. Let equivalence relation R_L be defined by: xR_Ly iff for all z in Σ^* xz is in L exactly when yz is in L. Then R_L is of finite index.

Myhill-Nerode Theorem

- Usefulness of Myhill-Nerode Theorem:
  - We have seen that a language will be accepted by two automata, but one will have less number of states than others. So, **how to minimize a DFA**, for that the idea in this theorem will be useful.
  - We used pumping lemma to show that certain languages are not regular. But in some cases it was not easy to prove using pumping lemma. For that reason we use this theorem to **show something is not regular**. So, another way of proving that something is not regular is by Myhill-Nerode Theorem.

Myhill-Nerode Theorem

- What is an equivalence relation ?
  - A relation is **equivalence relation** if it is reflexive, symmetric and transitive. So, if the three properties are satisfied it is called an equivalence relation.

$$\begin{array}{ll} xRx & \textit{reflexive Property} \\ xRy \Rightarrow yRx & \textit{symmetric Property} \\ xRy \wedge yRz \Rightarrow xRz & \textit{transitive property} \end{array}$$

Myhill-Nerode Theorem

- What is equivalence class and index of the equivalence relation ?
  - An equivalence relation partitions the underlined set into classes. The **number of equivalence classes** is known as the **index of the equivalence relation**.
    - ★ For example, if we consider the relation over the set of non-negative integers mod 3 relation, then we have three equivalence classes. Those that leaves the remainder 0, those that leave the remainder 1 and those that leave the remainder 2.
    - ★ Consider an automata with n states, say $q_0, q_1, \cdots, q_{n-1}$. The set of strings which take you from q_0 to q_0 belongs to one equivalence class, set of strings which take you from q_0 to q_1 belong to another class and so on. So, we have at most n equivalence classes. So, the number of equivalence classes will be at most the number of states of the automata.

Myhill-Nerode Theorem

- **Proof:** Let us prove this theorem. There are three statements. So, we will prove it as **1** implies **2**, **2** implies **3**, and **3** implies **1**. So that all of them are equivalent.

- **1** $\Rightarrow$ **2**: What we have to show that, the language L contained in Σ^* is accepted by some FSA implies that L is a union of some of the equivalence classes of a right invariant equivalence relation of finite index.
  Let L be accepted by a DFA $M = (Q, \Sigma, \delta, q_0, F)$ and we define an equivalence relation R_M on Σ^*.
  Two strings x and y related by R_M i.e., xR_My if $\delta(q_0, x) = \delta(q_0, y)$
  - Why do we say that this is an equivalence relation ?
    - It has to satisfy the three properties, reflexive, symmetric and transitive. But this itself is define using equality relation. So, equality relation has all the three properties, reflexive, symmetric and transitive. So, this is an equivalence relation.

  So, R_M is an equivalence relation. The index of R_M is at most the number of states of M.

Myhill-Nerode Theorem

- **1 ⇒ 2** contd..

  Now we have to show that, is this relation right invariant ?

  - What do we mean by right invariant ?
    - ⋆ If x is related to y, for any z, xz should be related to yz. Take any string if it is right invariant the underlying operation is concatenation. So, $xR_My \Rightarrow xzR_Myz$ for any z. Then we can say R_M is right invariant.

  This is very obvious. Suppose $\delta(q_0, x) = \delta(q_0, y)$ then

$$\begin{aligned}\delta(q_0, xz) &= \delta(\delta(q_0, x), z)\\ &= \delta(\delta(q_0, y), z)\\ &= \delta(q_0, yz)\end{aligned}$$

  So, R_M is right invariant.

  One more point is there, L is the union of some of the equivalence classes of that relation.

Myhill-Nerode Theorem

- **1 ⇒ 2** contd..

  So, this equivalence relation R_M, if there are n states, the equivalence classes I will call as $e_0, e_1, \cdots, e_i, \cdots, e_{n-1}$. Supposing all states are reachable from q_0. These are the equivalence classes, they are subset of Σ^*. Σ^* is partition into them.

$$\begin{array}{ccccc} e_0 & e_1 & e_i & e_r & e_{n-1} \\ | & | & | & | & | \\ q_0 & q_1 & q_i & q_r & q_{n-1} \end{array}$$

  e_i is a set of strings which take you from q_0 to q_i. Among these states some of them are final states. Let q_r is a final state. Then there will be a class corresponding to that, i.e., e_r. L is the union of such classes because L is a set of strings which take you from q_0 to a final state. So, among these classes, some of them will correspond to final states, take the union of them that will be L.

  So, what we have seen ? If we assume that L is accepted by a DFA with n states, then you can define a relation R_M. It is equivalence relation, it is right invariant, it is a finite index and L will be the union of some of those equivalence classes induced by this equivalence relation.

Myhill-Nerode Theorem

- **$2 \Rightarrow 3$**
  Let E be an equivalence relation as defined in **2**. That is, E is a equivalence relation on Σ^*, finite index, right invariant and L is a union of some of the equivalence classes. Then R_L is defined as given in **3**. We have to show that E is a refinement of R_L.
  - What is refinement ?
    - Let the equivalence relation R_1 which partitions the set into 5 equivalence classes. Consider another equivalence relation R_2 which partitions the set into 3 equivalence classes, like this
      R_1 — — — — —
      R_2 ——— — ———
      In R_1, this equivalence class of R_2 is divided into two, then you can say R_1 is a refinement of R_2. That is, one equivalence class of R_1 is completely contained in one equivalence class of R_2. Then you can say that R_1 is a refinement of R_2.

  Now, we have xEy, that is x and y belong to a same equivalence class of E. E is right invariant, so xz is related to yz for any z belong to Σ^* i.e., $xzEyz$.

Myhill-Nerode Theorem

- **2** $\Rightarrow$ **3** contd..
  Now, L is the union of some of the equivalence classes of E. So, if L contains this ($xzEyz$) equivalence class then xz and yz will both be in L.
  - L will contain one equivalence class completely or may not contain anything. It is not that portion of equivalence class it will contain and leave the remaining. L include one equivalence class completely or it exclude it. So, if L include this ($xzEyz$) equivalence class both xz and yz will be in L, if L does not include this ($xzEyz$) equivalence class xz and yz both will not be in L.

  So, for any z, either xz and yz both will be in L or xz and yz both will not be in L. This is the condition of R_L, xR_Ly iff for all z in Σ^* xz is in L exactly when yz is in L. So, that means if xEy holds the $xzEyz$ implies xR_Ly, x and y are also related by R_L.

Myhill-Nerode Theorem

- **2 ⇒ 3** contd..

  What does that mean, if x related to y by E, x is also related to y by R_L that means, one equivalence class of E is completely contained in one equivalence class of R_L. May be 2 equivalence class of E together form an equivalence class of R_L it may be possible. So, essentially x related to y by E means x is also related to y by R_L that is each equivalence class of E is completely contained in one equivalence class of R_L. That means, E is a refinement of R_L.

  What is the index of E ?
  We stated with the assumption that L is the union of some of the equivalence classes of a right invariant equivalence relation of finite index. So, we can say, E is of finite index.
  Index of $R_L \leq$ index of E. Because, every equivalence class of E is contained in one equivalence class of R_L. Therefore, R_L is of finite index.

Myhill-Nerode Theorem

- **$3 \Rightarrow 1$**
  First prove R_L is right invariant. How do we prove this ?
  The definition of R_L is xR_Ly if $xz \in L \Leftrightarrow yz \in L$
  Now instead of taking z, I take wz that is $xwz \in L \Leftrightarrow ywz \in L$ for all w and for all z. So, x whatever may be w and whatever may be z, xwz belongs to L implies equivalent to saying ywz belongs to L.
  So, we conclude that xw related to yw, i.e., xwR_Lyw.
  We started with xR_Ly and we come to xwR_Lyw. That means, R_L is right invariant.

  Now define an FSA $M^{'} = (Q^{'}, \Sigma, \delta^{'}, q_0^{'}, F^{'})$ as follows:
  - For each equivalence class of R_L we have a state in $Q^{'}$. So, the number of states of $Q^{'}$ is index of R_L.
  - $q_0^{'} = [\epsilon]$
    - $q_0^{'}$ is the equivalence class to which ϵ belongs. Empty string belong to one of the equivalence classes that equivalence class corresponds to a state and that is the initial state.

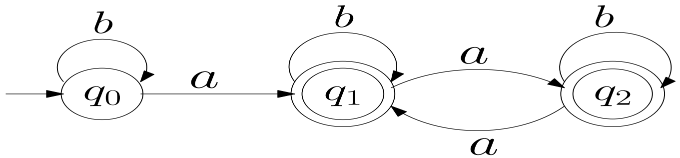
Myhill-Nerode Theorem

- **3 $\Rightarrow$ 1** contd..
  - $\delta^{'}([x], a) = [xa]$
    - $[x]$ is an equivalence class, the state which represents the equivalence class to which x belongs. Then after reading a symbol a to which state does it go. It goes to the state xa.
  - $F^{'} = \{[x] | x \in L\}$
    - $F^{'}$ corresponds to those states some equivalence classes will be in L. So, make those states as final states.

Assuming **3** that is: we are defining an equivalence relation R_L such that xR_Ly iff for all $z \in \Sigma^*$ xz is in L exactly when yz is in L and R_L is finite index. Then we show that it can be accepted by a FSA.

Myhill-Nerode Theorem

- **Example:** We illustrate these three proof by an example



- This is a DFA and it has three states.
- The language accepted by this machine: any string having at least one a will be accepted. A sequence of b will not be accepted.
- So, Σ^*, we can divide into three equivalence classes J_0, J_1 and J_2.
  - J_0 corresponds to strings which take you from q_0 to q_0
  - J_1 corresponds to strings which take you from q_0 to q_1
  - J_2 corresponds to strings which take you from q_0 to q_2

  For example

J_0	J_1	J_2
ϵ	a	aa
b	ba	aba
bb	bab	$babab$

Myhill-Nerode Theorem

- If we look it carefully, set of strings which do not contain an a at all will belong to class J_0, just strings of b's alone. Any string having an odd number of a's will be in J_1. Any string having even number of a's will be in J_2. So, Σ^* is partition into three classes.
- Now $L = J_1 \cup J_2$
- So, we can see that staring with a DFA, we find that it divide Σ^* into equivalence classes with finite index. Here, index is three. And, L is the union of some of the equivalence classes.
- If two string x and y belong to same class, then xz and yz will also belong to the same equivalence class. So, it is right invariant and L is the union of two equivalence class, i.e., $J_1 \cup J_2$.
- R_M:

	J_0	J_1	J_2
	b	a	aa

Myhill-Nerode Theorem

- Now, how they are related by R_L ? How we define R_L like this, i.e., xR_Ly iff for z in Σ^* xz is in L exactly when yz is in L.
- In R_L, number of equivalence classes can not be more than three. It can be three, it can be two or it can be one. So, we have to find out whether two of the equivalence classes can be grouped for R_L.

J_0	J_1		J_0	J_2
b	a		b	aa
bb	ab		bb	aab

- Take J_0 and J_1. Take b and a. Take z as b. Then,bb is not in L but ab in L. So, J_0 and J_1 are cannot be same equivalence classes for R_L
- Take J_0 and J_2. Take b and aa. Take z as b.bb not in L but aab in L. So, J_0 and J_2 are cannot be same equivalence classes for R_L

Myhill-Nerode Theorem

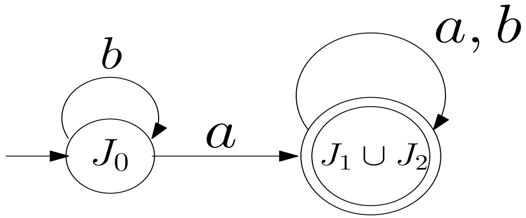
- Now, take two string string in J_1 and J_2. Say w_1 and w_2. Take any z

J_1	J_2
w_1	w_2
$w_1 z$	$w_2 z$

  After reading z either you will be in q_1 or q_2, you cannot go back to q_0. After reading w_1 you are in q_1, after reading z you will be in q_1 or q_2. So, $w_1 z$ will be accepted. Similarly, staring from q_0 after reading w_2 you are in q_2, then read z you will be either in q_1 or q_2. So, that will also accepted. So, whatever may be z in this case $w_1 z$ and $w_2 z$ will be accepted. So, we can group them together. J_1 and J_2 can be group together. R_L has only two equivalence classes, J_0 and $J_1 \cup J_2$. Index of R_L is two.
  R_L: J_0 $J_1 \cup J_2$

Myhill-Nerode Theorem

- Now, we have seen that R_L has two equivalence classes. So, if we want to construct a finite automata, it will have two states. One state will be J_0 and another will be $J_1 \cup J_2$.



ϵ belongs to J_0, so J_0 will be the initial state.

Myhill-Nerode Theorem

- Use Myhill-Nerode Theorem to show that $L = \{a^n b^n : n \geq 1\}$ is not regular ?

  We have used pumping lemma to show that this is not regular. Now, we want to show that this is not regular by using the Myhill-Nerode theorem.

- **Proof:**
  - Suppose L is regular. Then by Myhill-Nerode theorem, L is the union of some of the equivalence classes of a right invariant equivalence relation of finite index. So, that equivalence relation divide Σ^* into equivalence classes and they are finite.
  - Now, consider the strings $a, a^2, a^3, a^4, \cdots$, they are all belonging to Σ^*. Now, each one cannot be in different equivalence class because the number of equivalence classes is finite.
  - So, for example a^m and a^n are in a same equivalence class, where $m \neq n$.

Myhill-Nerode Theorem

- **Proof Contd:**
  - Now, because of right invariant $a^m b^m$ and $a^n b^m$ will be in the same equivalence class.
  - Now, L will contain one equivalence class completely or it will not contain that equivalence class.
  - Now, $a^m b^m \in L$, but L should contain the whole equivalence class. So, $a^n b^m$ also belongs to L where $n \neq m$.
  - This is a contradiction, because the language is only $a^n b^n$, equal number of a's followed by equal number of b's. So, we are arriving at a contradiction. Therefore, L is not regular.