Notes on Myhill-Nerode Theorem

Euan Mendoza

Sunday the 12th of November, 2023

Contents

1 Introduction

Myhill-Nerode Theorem relates regular languages and equivalence classes. It is an incredibly powerful way to prove that a language is or is not regular. There is already an abundant amount of resources which prove the Myhill-Nerode Theorem so here I focus on showing *examples* of the Myhill-Nerode Theorem.

In order to describe Myhill-Nerode's theorem we first need to describe the notion of a *distinguishable* and *indistinguishable* string.

Definition 1.1. Given a alphabet Σ, let L be a language over Σ^*. The words $x, y \in \Sigma^*$ are *indistinguishable* by L (denoted $x \equiv_L y$) if and only if for every word $z \in \Sigma^*$ either $xz \in L$ and $yz \in L$ or both $xz \notin L$ and $yz \notin L$. It should be trivial to show that $\equiv_L$ is an equivalence relation for the language L.

It is also important to note the distinct difference between equality $x = y$, an equivalence relation $x \equiv_L y$ and an *equivalence class*. An equivalence class is not *strictly* equal but has the same properties of things being equal. We can use *equivalence relations* to partition sets, and in this case we can use the *indistinguishable* relation to partition our language into subsets of the language where every word in the subset is *indistinguishable*. These are called *equivalence classes* and are vitally important to understanding Myhill-Nerode.

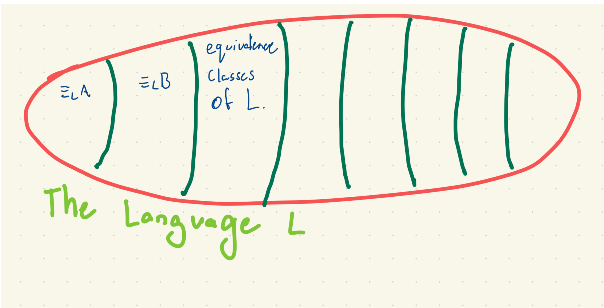

Figure 1: Equivalence Class Partitions on the Language L

This leads to the following important notion.

Definition 1.2. Given a alphabet Σ, let L be a language over Σ^*. The words $x, y \in \Sigma^*$ are *distinguishable* by L if and only if there exists a word $z \in \Sigma^*$ such that $xz \in L$ and $yz \notin L$ or vice-versa.

Note that the above is the direct opposite definition to a word being *indistinguishable*.

Lemma 1.1. *The number of equivalence classes is the same as the number of distinguishable words in a language.*

Proof. If two words are distinguishable with respect to a language L, then by definition they are not indistinguishable with each other. Hence they must be in different equivalence classes. It follows that every distinguishable word forms a separate equivalence *class* (note this is not the same as an equivalence relation). ■

2 Myhill-Nerode Theorem

We now have enough information to formally state the Myhill-Nerode theorem.

Theorem 1 (Myhill-Nerode)**.** *A language L is regular if and only if $\equiv_L$ has a finite number of equivalence classes.*

This has the important counter definition which is very helpful in proving that a language *is not* regular.

Corollary 1.1. *If there exists an infinite number of distinguishable words in a set with respect to $\equiv_L$ for a language L, then L is not regular.*

Proof. By Lemma 1.1, if an infinite number of words *distinguish* a language L, then the number of equivalence classes is infinite. By Myhill-Nerode Theorem, if a language has an infinite number of equivalence classes it cannot be regular. ∎

Example 1.1. *Prove the language $L_a = \{0^n 1^m 0^n \mid n, m \in \mathbb{N}\}$ is not regular.*

Proof. Let $S = \{0^n 1 \mid n \in \mathbb{N}\}$ be an infinite set of words. For $i, j \in \mathbb{N}$ where $i \neq j$, consider the string 0^i, for the string $0^i 1 \in S$ and $0^j 1 \in S$, the string $0^i 1 0^i \in L_a$ and $0^j 1 0^i \notin L_a$ for every i in $\mathbb{N}$. As such, there is an infinite number of distinguishable strings with respect to L_a, hence there is an infinite number of equivalence classes under $\equiv_{L_a}$ so L_a cannot be regular. ∎

Example 1.2. *Prove the language $L_b = \{0^i 1^j 0^k \mid i, j, k \in \mathbb{N}, i = j$ or $j = k\}$ is not regular.*

Proof. Let $S = \{a^n b^{n+1} \mid n \in \mathbb{N}\}$ be an infinite set of words. For $i, j \in \mathbb{N}$ where $i \neq j$, consider the string c^{i+1}, for the string $a^i b^{i+1} \in S$ and $a^j b^{j+1} \in S$, the string $a^i b^{i+1} c^{i+1} \in L_b$ and $a^j b^{j+1} c^{i+1} \notin L_b$ for every i in $\mathbb{N}$. As such, there is an infinite number of distinguishable strings with respect to L_b, hence there is an infinite number of equivalence classes under $\equiv_{L_b}$ so L_b cannot be regular. ∎

Example 1.3. *Prove the language $L_c = \{ww^R \mid w \in \{0, 1\}^*\}$ is not regular.*

Proof. Let $S = \{0^n 1 \mid n \in \mathbb{N}\}$ be an infinite set of words. For $i, j \in \mathbb{N}$ where $i \neq j$, consider the string 10^i, for the string $0^i 1 \in S$ and $0^j 1 \in S$, the string $0^i 1 1 0^i \in L_c$ and $0^j 1 1 0^i \notin L_c$ for every i in $\mathbb{N}$. As such, there is an infinite number of distinguishable strings with respect to L_c, hence there is an infinite number of equivalence classes under $\equiv_{L_c}$ so L_c cannot be regular. ∎

Notice the general strategy used here was to find an infinite set of strings such that every string in the set was distinguishable. This implied that number of equivalence classes is also infinite and by Myhill-Nerode the language could not be regular.

A Appendix

A.1 A brief note regarding infinity

Usually we use infinity to denote the *size* of a set. Usually a set can either be *finite* or *infinite*.

Definition A.1. Let $[n] = \{1, 2, \ldots, n\}$. A set S is *finite* with a size n if there exists a bijective function $f : S \to [n]$.

Recall that a bijective function is a *invertible function* or equivalently that it is both *surjective* and *injective*.

Definition A.2. Given a function $f : X \to Y$ which maps X to Y, f is bijective if and only if it is both

1. *injective:* $\forall x, x' \in X, f(x) = f(x') \implies x = x'$.
2. *surjective:* $\forall y \in Y, \exists x \in X, f(x) = y$.

Finally we can say is infinite if there exists a *injective* function from $S \to \mathbb{Z}$ and if the function is also a bijection we say it is *countably infinite*.