Myhill–Nerode Theorem

Based on slides of Aaron Deever

Minimizing DFAs

- Given a language, L, what's the minimal size DFA that can recognize it?
  - So far, we've taken descriptions of languages and built DFAs from them, but with no idea if the DFAs are unnecessarily large
  - Now we'll look at Myhill-Nerode theorem discussing the minimal size of a DFA recognizing a language L
  - We'll also describe an algorithm for reducing a DFA to a minimal form (this is separate from Myhill-Nerode)
  - This will also help answer the question: given two different DFAs, do they recognize the same language?

Minimal DFA

- For a language L, we'll define a Minimal Finite Automaton to be a DFA with the fewest states that recognizes L
- To answer the question:
  - Do two finite automata accept the same language?
  - We can generate the MFA for each DFA, then compare the MFAs on a state by state basis.

Distinguishability

- Let x, y be strings, and let L be a language
- x and y are **<u>distinguishable by L</u>** if
  - There exists a string z such that
    - $xz \in L$ and $yz \notin L$ or vice versa.
- x and y are **<u>indistinguishable by L</u>** if
  - For all strings z either
    - $xz \in L$ and $yz \in L$ or
    - $xz \notin L$ and $yz \notin L$

z can be the empty string ε

Example

- Sipser Example 1.30 and Figure 1.32
- A is the language of all strings over {0,1} containing a 1 in the third position from the end
  - Show that 000 and 111 are distinguishable by **A.**
  - Show that 000 and 001 are distinguishable by **A.**
  - Show that 000 and 010 are distinguishable by **A.**

Transition Function on Strings

- What does distinguishability have to do with DFAs?
  - Let M = (Q, Σ, δ^*, q_0, F) be a DFA recognizing language L
- Applying the transition function to a string.
  - δ^* is a function from Q x Σ^* to Q
  - $\delta^*(q, x) = q'$ where
    - $q, q' \in Q$
    - $x \in \Sigma^*$
  - δ^* defines, given a current state *q* and reading a string *x*, to which state the DFA will move once all characters of x are read.

Transition Function on Strings

- What does distinguishability have to do with DFAs?
  - Let $M = (Q, \Sigma, \delta^*, q_0, F)$ be a DFA recognizing language L
  - Let x and y be distinguishable by L
  - Then what must be true about $\delta^*(q_0,x)$ and $\delta^*(q_0,y)$?
    - They must be different states

Example Continued

- Let X = {000,001,010,011,100,101,110,111}
- Show that X is pairwise distinguishable by A
  - Every two distinct strings in X are distinguishable by A
  - Show this by appending symbols on the end of each as necessary until one string has a 1 in the third from last position, and the other doesn't
  - Why is this possible for all elements of X?
    - All 8 elements of X differ from each other in at least one of the three locations
      - To show distinguishability, just add 0,1 or 2 symbols as necessary to get the differing spot to be 3rd from the end

Example Continued

- Now let M be a DFA for language A
- M must have at least 8 states
  - Why?
  - Suppose M had fewer than 8 states
    - What could we say about the strings of X
    - $\delta^*(q_0,x)$ and $\delta^*(q_0,y)$ would have to be the same state for at least two elements $x,y \in X$
    - But this contradicts the distinguishability of the strings in X
  - So the pairwise distinguishability says something about the minimum size of the DFA…

Myhill-Nerode Theorem

- Definition: the index of a language L is the maximum number of elements in any set that is pairwise distinguishable by L
- Myhill-Nerode Theorem (Problem 1.52.c)
  - L is regular if and only if it has finite index. Moreover, its index is the size of the smallest DFA accepting it.

Myhill–Nerode Theorem

- We will show this theorem follows from Problems 1.52.a and 1.52.b

- Problem 1.52.a:
  - If L is accepted by a DFA with k states, then L has index at most k.

- Problem 1.52.b:
  - If the index of L is a finite number k, then L is accepted by a DFA with k states.

Myhill–Nerode Theorem

- Part 1: If L is accepted by a DFA with k states, then L has index at most k.
  - We've shown this already in our example.
  - If the index of L were greater than k, then by the pigeonhole principle there must be at least two pairwise distinguishable strings that end up in the same state
    - $\delta^*(q_0,x) = \delta^*(q_0,y)$
      - But then they aren't distinguishable

- What does this say about the language L in the case when the index of L is infinite?
  - It is NOT regular

Brief Tangent

- This idea can be used to show that the language $L = \{a^i b^i \mid i \geq 0\}$ is not regular
- How?
  - Can we show that the index of L is infinite?
  - Consider $X = \{a^i \mid i \geq 0\}$
    - Any two elements of X are pairwise independent
    - Take the string z to be b^i where i is the exponent of one of the two elements of X being compared

Myhill–Nerode Theorem

- Part 2: If the index of L is a finite number k, then L is accepted by a DFA with k states.

- First, recall that strings x and y are <u>**indistinguishable by L**</u> if
  - For all strings z either
    - $xz \in L$ and $yz \in L$ or
    - $xz \notin L$ and $yz \notin L$
- We write $x \equiv_L y$
- For every language L, $\equiv_L$ is an equivalence relation
- Note that the index of L is equal to the number of equivalence classes for the relation $\equiv_L$

Equivalence Classes

- **Example**: find the equivalence classes for the relation $\equiv_L$ when:
  - $L = \{0w \mid w \in \{0,1\}^*\}$

Equivalence Classes

- **Example:** find the equivalence classes for the relation $\equiv_L$ when:
  - L = {0w | w ∈ {0,1}*}
    - $[0]_{\equiv_L}$: all strings beginning with a 0
    - $[1]_{\equiv_L}$: all strings beginning with a 1
    - $[\varepsilon]_{\equiv_L}$: ε

Equivalence Classes

- **Example**: find the equivalence classes for the relation $\equiv_L$ when:
-
  - L = {w ∈ {0,1}* | number of 1's in w is div. by 3}

Equivalence Classes

- **Example**: find the equivalence classes for the relation $\equiv_L$ when:
-
  - L = {w ∈ {0,1}* | number of 1's in w is div. by 3}
    - $[0]_{\equiv_L}$: all strings with number of 1's mod 3 = 0
    - $[1]_{\equiv_L}$: all strings with number of 1's mod 3 = 1
    - $[2]_{\equiv_L}$: all strings with number of 1's mod 3 = 2

Myhill–Nerode Theorem

- Part 2: If the index of L is a finite number k, then L is accepted by a DFA with k states.
- What we know so far:
  - Given index equal to k, any DFA for L is going to need at least k states
  - Given index equal to k, there are k equivalence classes associated with the $\equiv_L$ relation
  - For a given equivalence class, all the strings in the class "behave the same" from that point forward with respect to being accepted by a DFA recognizing L.
    - We just need to argue that we only need 1 state to represent all of the strings of a particular equivalence class.
      - Show that we can build a DFA that recognizes L such that all the strings of a given equivalence class land you in one state.

Myhill-Nerode Theorem

- Part 2: If the index of L is a finite number k, then L is accepted by a DFA with k states.
- Let $X = \{s_1, \ldots, s_k\}$ be pairwise distinguishable by L. We define a k-state DFA M that accepts L as follows.
- $M = (Q, \Sigma, \delta^*, q_0, F)$ where
  - $Q = \{q_1, \ldots, q_k\}$
  - $\delta^*(q_i, w) = q_j$ where $s_j \equiv_L s_i w$ for $w \in \Sigma^*$
  - $q_0 = q_i$ where $s_i \equiv_L \varepsilon$
  - $F = \{q_i \mid s_i \in L\}$

Myhill–Nerode Theorem

- One can show that in this construction, for every state q_i,
  - $\{w \mid \delta^*(q_0, w) = q_i\} = \{w \mid w \equiv_L s_i\}$
  - This implies that L(M) = L
  - I will step through this, but don't worry too much about the details

Myhill–Nerode Theorem

- Why is $\{w \mid \delta^*(q_0, w) = q_i\} = \{w \mid w \equiv_L s_i\}$?
  - Suppose $\delta^*(q_0, w) = q_i$
    - Then $s_i \equiv_L s_k w$ by construction where $s_k \equiv_L \varepsilon$
    - But if two strings are L–equivalent, we can concatenate a string to each and they are still L–equivalent, so
    - $s_k w \equiv_L \varepsilon w$
    - $s_k w \equiv_L w$
    - By equivalence (transitivity) $s_i \equiv_L w$
  - (other direction is similar)

Myhill-Nerode Theroem

- Why does this imply L(M) = L
  - Suppose $w \in L$
  - We know $w \equiv_L s_i$ for some i by index property
  - Then $s_i \in L$ because $w\varepsilon$ and $s_i\varepsilon$ must both be in or out
  - By shown relationship, $\delta^*(q_0, w) = q_i$
  - But $F = \{q_i \mid s_i \in L\}$ so q_i is accepting and M accepts string w
  - Now go the other way and assume w is accepted by M
  - (similar approach)

Myhill-Nerode Concepts

- A language L has an index, which is the maximal size of any set, X, of pairwise distinguishable strings.
- L is regular if and only if the index is finite.
- For language L, $\equiv_L$ defines an equivalence relation.
- The size of an index set X equals the number of equivalence classes. Each element of index set X belongs to a different equivalence class.
- Each equivalence class represents all strings that are indistinguishable from one another with respect to language L.
- Each equivalence class c_i corresponds to a unique state q_i in the minimal DFA. Running any string from c_i through the minimal DFA lands you in q_i.

Extra Example: Using Myhill-Nerode to Prove Nonregularity

- Show $L = \{ww^R \mid w \in \{0,1\}^*\}$ is not regular

Example Problem

- $L = \{ w \in \{a,b\}^* \mid w \text{ contains substring abb}\}$
  - What is a minimal DFA? (draw a DFA you think might be minimal)
  - What is the value of the index of L?
  - What is an index set X of pairwise distinguishable strings?
    - Show they are distinguishable
  - Give a RE for each equivalence class of $\equiv_L$
    - Read off a RE for how you can end up in each state

Computing a Minimal DFA

- While Myhill-Nerode can be used to construct a minimal DFA for a given language L…
- … in general it can be difficult to derive an index set X of pairwise distinguishable strings to work from for an arbitrary language L
- Instead – we will use an algorithmic approach to take a DFA as a starting point, and minimize it.