Myhill-Nerode theorem

Atri Rudra

April 26

Announcements

- Handout
  - Solutions to HW# 3
- Pick up handout on DFA minimization
  - If you did not do so last class

Errata for Soln to HW #3

- Solution to 3(b) is the solution for 3(a)
- Solution for 3(b) is the following
  - \( 1(\Sigma \Sigma)^* \cup 010(\Sigma \Sigma \Sigma)^* \)

Puzzle

- Prove that any DFA for the following language has at least \(2^{k-1}\) states
  - \( L_k = \{ w | w \in \{0,1\}^*, k^{th} \text{ last symbol of} \ w \ \text{is a} \ 1 \} \)

Stuff from last lecture

- Given DFA \( M = (Q,\Sigma,\delta,s,F) \)
- Strings \( x,y \in \Sigma^* \) are indistinguishable by \( M \)
  - \( x \equiv_M y \)
  - \( x \) and \( y \) end up in the same state in \( M \) (from \( s \))

Another equivalence relation

- Given a language \( A \) over \( \Sigma \)
- String \( x, y \in \Sigma^* \) are indistinguishable
  - \( x \equiv_A y \)
  - For all \( z \in \Sigma^* \), \( xz \in A \iff yz \in A \)
What is the relation b/w $\equiv_M$ and $\equiv_A$?

- Let $M$ be a DFA such that $A = L(M)$
- If $x \equiv_M y$ then $x \equiv_A y$
- Basic intuition:
  - Once $x$ and $y$ have been consumed, both reach the same state (say $q$)
  - Thus for any $z$, the path followed by $xz$ and $yz$ after $q$ would be the same

If $x \equiv_M y$ then $x \equiv_A y$

- Any equivalence class in $\equiv_A$ is union of equivalence classes in $\equiv_M$
  - An eqv class in $\equiv_A$ could be the same as one in $\equiv_M$

Some implications

- $\#\text{ eqv classes in } \equiv_A \leq \#\text{ eqv classes in } \equiv_M$
  - For any $M$ such that $A = L(M)$
- If $A$ is regular then $\equiv_A$ has finite # of eqv classes
  - Consider any DFA $M$ such that $A=L(M)$

Proving languages are not regular

- If $\equiv_A$ has infinite eqv classes then $A$ is not regular
- What is the “method”?
  - Find an infinite sequence of strings $x_1,x_2,...$
  - For any $x_i$ and $x_j$, $x_i \not\equiv_A x_j$
  - Find a string $z_{ij}$ such that $x_i z_{ij} \in A$ but $x_j z_{ij} \not\in A$
  - Recall $x_i \equiv_A x_j$ iff for all $z$, $x_i z \in A$ if and only if $x_j z \in A$

An example

- $A = \{ 0^n1^n | n \geq 0 \}$
- Let $x_i = 0^i$, $i=1,2,...$
- Need to show $x_i$ and $x_j$ are not equivalent
  - $z_{ij} = 1^j$
  - $x_i z_{ij} = 0^i1^j \in A$, but
  - $x_j z_{ij} = 0^i1^j \not\in A$

Questions?
Myhill-Nerode theorem

- A is regular ⇔ \( \equiv_A \) has finite number of equiv classes
- \( \equiv \) we have seen
- ⇐ by construction
  - Build a DFA where each class gets its own state
  - Note that it will be the minimized DFA

Constructing a DFA from \( \equiv_A \)

- One state per equiv class
- Start state: class containing \( \varepsilon \)
- Final state(s): equiv class contained in \( A \)

Transitions

- If \( x \equiv_A y \) then \( xa \equiv_A ya \), \( a \in \Sigma \)
  - For all \( z \in \Sigma^* \), \( xz \in A \Rightarrow yz \in A \)
  - In particular for all \( z' \in \Sigma^* \), \( x(z') \in A \Rightarrow y(z') \in A \)
- For any equiv class and \( a \in \Sigma \), pick \( x \) and send the transition to equiv class containing \( \delta(x,a) \)

Constructing DFA w/ minimum states

- We know the minimized DFA has number of states equal to the number of classes in \( \equiv_A \)
- Given \( \equiv_A \), we know how to construct a DFA
- Hence, done?

There is a catch…

Minimizing DFAs

- We might not know \( \equiv_A \)
- Might only know the DFA that accepts \( A \)