CS310M: Automata Theory (Minor)

Topic 7: Myhill Nerode Theorem

Paritosh Pandya

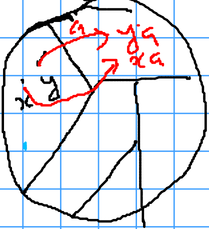
Indian Institute of Technology, Bombay
Course URL: https://cse.iitb.ac.in/∼pandya58/CS310/automata.html

Autumn, 2023

Myhill-Nerode Relations

Let $\equiv$ be an equivalence relation over Σ^*.

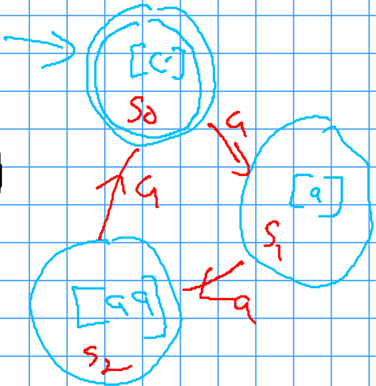
Σ^*



$x \equiv y$

$\Sigma = \{a\}$

$(aaa)^*$, $(aaa)^*a$, $(aaa)^*aa$



Let $\equiv$ be an equivalence relation over Σ^*.

- $\equiv$ is right congruent if $\forall x, y \in \Sigma^*,\ a \in \Sigma$ we have
$$x \equiv y \quad \Rightarrow \quad x \cdot a \equiv y \cdot a$$

Myhill-Nerode Relations

Let $\equiv$ be an equivalence relation over Σ^*.

- $\equiv$ is right congruent if $\forall x, y \in \Sigma^*,\ a \in \Sigma$ we have
  $$x \equiv y \quad \Rightarrow \quad x \cdot a \equiv y \cdot a$$
- Let $R \subseteq \Sigma^*$ (not necessarily regular).
  $\equiv$ refines R if $\forall x, y \in \Sigma^*$
  $$x \equiv y \quad \Rightarrow \quad (x \in R \Leftrightarrow y \in R)$$

Σ $\quad x \equiv y$ iff $x = y$.

Myhill-Nerode Relations

Let $\equiv$ be an equivalence relation over Σ^*.

- $\equiv$ is right congruent if $\forall x, y \in \Sigma^*,\ a \in \Sigma$ we have
$$x \equiv y \quad \Rightarrow \quad x \cdot a \equiv y \cdot a$$
- Let $R \subseteq \Sigma^*$ (not necessarily regular).
$\equiv$ refines R if $\forall x, y \in \Sigma^*$
$$x \equiv y \quad \Rightarrow \quad (x \in R \Leftrightarrow y \in R)$$
- $\equiv$ is of finite index if $\equiv$ partitions the Σ^* into only finitely many equivalence classes.

Myhill-Nerode Relations

Let $\equiv$ be an equivalence relation over Σ^*.

- $\equiv$ is right congruent if $\forall x, y \in \Sigma^*,\ a \in \Sigma$ we have
  $$x \equiv y \quad \Rightarrow \quad x \cdot a \equiv y \cdot a$$
- Let $R \subseteq \Sigma^*$ (not necessarily regular).
  $\equiv$ refines R if $\forall x, y \in \Sigma^*$
  $$x \equiv y \quad \Rightarrow \quad (x \in R \Leftrightarrow y \in R)$$
- $\equiv$ is of finite index if $\equiv$ partitions the Σ^* into only finitely many equivalence classes.

Myhill Nerode Relations

- Equivalence relation $\equiv$ is called Myhill-Nerode Relation refining R if it satisfies all the three properties above.
- $\equiv$ is called Weak Myhill Nerode relation Refining R if it satisifies the first two properties.

$\{(aaa)^*, \quad (aaa)^* a, \quad (aaa)^* aa\}$ $\quad \Sigma = \{a\}$

$R = \{w \mid w = 0 \bmod 3\}$

$R = \{ w \mid \#a(w) = 0 \bmod 6 \}$

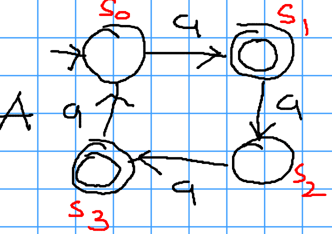
$(aaa)^*$

$(aaa)^* a$

$(aaa)^* aa$

Given a DFA $A = (Q, \Sigma, \delta, q_0, F)$ define the induced equivalence $\equiv_A$ over Σ^* as follows:

$$x \equiv_A y \quad \stackrel{\text{def}}{=} \quad \hat{\delta}(q_0, x) = \hat{\delta}(q_0, y).$$



$a, aaa, aaaaa, \ldots \in L(A)$

$a \equiv_A aaaaa$ why?

$\hat{\delta}(s_0, a) = s_1$ $\hat{\delta}(s_0, aaaaa) = s_1$

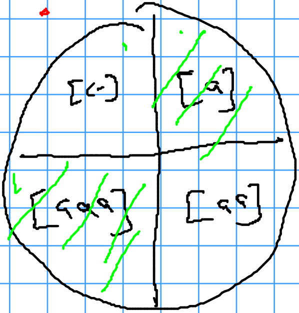
$a \not\equiv_A aa$!

$s_0 \mapsto (aaaa)^* = [\epsilon]$

$s_1 \mapsto (aaaa)^* a = [\epsilon] \cdot a$ ✓

$s_2 \mapsto (aaaa)^* aa = [\epsilon] \cdot aa$

$s_3 \mapsto \underset{aaa}{(aaaa)^*} = [\epsilon] \cdot aaa$ ✓



Machine Equivalence

Given a DFA $A = (Q, \Sigma, \delta, q_0, F)$ define the induced equivalence $\equiv_A$ over Σ^* as follows:

$$x \equiv_A y \quad \stackrel{\text{def}}{=} \quad \hat{\delta}(q_0, x) = \hat{\delta}(q_0, y).$$

Proposition $\equiv_A$ is a Myhill-Nerode relation refining $L(A)$.

Machine Equivalence

Given a DFA $A = (Q, \Sigma, \delta, q_0, F)$ define the induced equivalence $\equiv_A$ over Σ^* as follows:

$$x \equiv_A y \quad \stackrel{\text{def}}{=} \quad \hat{\delta}(q_0, x) = \hat{\delta}(q_0, y).$$

Proposition $\equiv_A$ is a Myhill-Nerode relation refining $L(A)$.

Proof Method Check the following:

(a) $\equiv_A$ is an equivalence relation over Σ^*. ✓

(b) $x \equiv_A y \quad \Rightarrow \quad \forall a.\;\; xa \equiv_A ya.$ ✓

(c) $x \equiv_A y \quad \Rightarrow \quad x \in L(A) \quad \Leftrightarrow \quad y \in L(A)$

(d) $\equiv_A$ is of finite index.

Right Congruence

Refining L(A)

Given a DFA $A = (Q, \Sigma, \delta, q_0, F)$ define the induced equivalence $\equiv_A$ over Σ^* as follows:

$$x \equiv_A y \quad \stackrel{\text{def}}{=} \quad \hat{\delta}(q_0, x) = \hat{\delta}(q_0, y).$$

Proposition $\equiv_A$ is a Myhill-Nerode relation refining $L(A)$.

Proof Method Check the following:
(a) $\equiv_A$ is an equivalence relation over Σ^*.
(b) $x \equiv_A y \quad \Rightarrow \quad \forall a.\ \ xa \equiv_A ya$.
(c) $x \equiv_A y \quad \Rightarrow \quad x \in L(A) \quad \Leftrightarrow \quad y \in L(A)$
(d) $\equiv_A$ is of finite index.

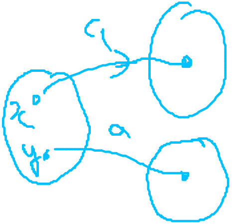
Example: We give automaton A and the induced equivalence partitions.

From Equivalence to DFA

Let $\equiv$ be Myhill-Nerode refining R. Define DFA $A_{\equiv} \stackrel{\text{def}}{=} (Q, \Sigma, \delta, q_0, F)$ as follows:

$$Q \stackrel{\text{def}}{=} \{[x] \mid x \in \Sigma^*\}$$
$$q_0 \stackrel{\text{def}}{=} [\epsilon]$$
$$F \stackrel{\text{def}}{=} \{[x] \mid x \in R\}$$
$$\delta([x], a]) \stackrel{\text{def}}{=} [xa]. \checkmark$$

(Check well-formedness.)



Let $\equiv$ be Myhill-Nerode refining R. Define DFA $A_{\equiv} \stackrel{\text{def}}{=} (Q, \Sigma, \delta, q_0, F)$ as follows:

$$Q \stackrel{\text{def}}{=} \{[x] \mid x \in \Sigma^*\}$$
$$q_0 \stackrel{\text{def}}{=} [\epsilon]$$
$$F \stackrel{\text{def}}{=} \{[x] \mid x \in R\}$$
$$\delta([x], a]) \stackrel{\text{def}}{=} [xa].$$

(Check well-formedness.)

Theorem $L(A_{\equiv}) \quad = \quad R.$

From Equivalence to DFA

Let $\equiv$ be Myhill-Nerode refining R. Define DFA $A_{\equiv} \stackrel{\text{def}}{=} (Q, \Sigma, \delta, q_0, F)$ as follows:

$$Q \stackrel{\text{def}}{=} \{[x] \mid x \in \Sigma^*\}$$
$$q_0 \stackrel{\text{def}}{=} [\epsilon]$$
$$F \stackrel{\text{def}}{=} \{[x] \mid x \in R\}$$
$$\delta([x], a]) \stackrel{\text{def}}{=} [xa].$$

(Check well-formedness.)

Proof

$x \in L(A_{\equiv})$

$\Leftrightarrow \hat{\delta}([\epsilon], x) \in F$

$\Leftrightarrow [\epsilon \cdot x] \in F$

$\Leftrightarrow x \in R$

Theorem $L(A_{\equiv}) = R.$

Lemma $\hat{\delta}([x], y) = [xy].$

Proof: Ind. on y.

Base ($y = \epsilon$) $\hat{\delta}([x], \epsilon) = [x] = [x \cdot \epsilon]$

cont.

Ind step $y = za$

$$\hat{\delta}([x], za) = \delta(\hat{\delta}([x], z), a)$$
$$= \delta([xz], a) \quad \text{Hyp}$$
$$= [xza] \quad \text{Def } \delta.$$

Correspondence

$$\equiv \xrightarrow{\text{aut}} A_{\equiv} \xrightarrow{\text{equ}} \equiv_{(A_{\equiv})}$$

The $\equiv_A$ and $A_{\equiv}$ are inverses of each other.

Theorem $\equiv_{A_{\equiv}} \quad = \quad \equiv$.

Theorem If A is automaton without unreachable states then $A_{\equiv_A}$ is isomorphic to A.

$$A \xrightarrow{\text{equn}} \equiv_A \xrightarrow{\text{aut}} A(\equiv_A)$$

Refining Equivalences

- Definition An equivalence relation $\equiv_1$ refines equivalence relation $\equiv_2$ provided $x \equiv_1 y \quad \Rightarrow \quad x \equiv_2 y$.

Refining Equivalences

- Definition An equivalence relation $\equiv_1$ refines equivalence relation $\equiv_2$ provided $x \equiv_1 y \quad \Rightarrow \quad x \equiv_2 y$.
- Set theoretically, $\equiv_1$ refines $\equiv_2$ provided $\equiv_1 \subseteq \equiv_2$.

Refining Equivalences

- Definition An equivalence relation $\equiv_1$ refines equivalence relation $\equiv_2$ provided $x \equiv_1 y \quad \Rightarrow \quad x \equiv_2 y$.
- Set theoretically, $\equiv_1$ refines $\equiv_2$ provided $\equiv_1 \subseteq \equiv_2$.
- $\equiv_1 \subseteq \equiv_2$ means $\equiv_1$ makes finer partitions compared to $\equiv_2$.

$N = \{0, 1, 2 \cdots\}$ $\quad x \equiv_i y$ iff $x = y \bmod i$

$\equiv_6 \ \langle [0], [1], [2], [3], [4], [5] \ \ \{0, 6, 12, 18 \cdots\} \ \{1, 7, 13, 19, \cdots\}$

$\equiv_6 \subseteq \equiv_3$

$\equiv_3 \ \langle [0], [1], [2] \ \ \{0, 3, 6, 9, 12, \cdots\} \ \{1, 4, 7, 10 \cdots\}$

Language Induced Equivalence (Nerode Congruence)

Given a language R (not necessarily regular), we extract an equivalence relation $\equiv_R$ from it.

Language Induced Equivalence (Nerode Congruence)

Given a language R (not necessarily regular), we extract an equivalence relation $\equiv_R$ from it.

Definition

Given $R \subseteq \Sigma^*$,

$$x \;\equiv_R\; y \quad \stackrel{\text{def}}{=} \quad \forall z \in \Sigma^*.\;\; (xz \in R \Leftrightarrow yz \in R).$$

Language Induced Equivalence (Nerode Congruence)

Given a language R (not necessarily regular), we extract an equivalence relation $\equiv_R$ from it.

Definition

Given $R \subseteq \Sigma^*$,

$$x \equiv_R y \stackrel{\text{def}}{=} \forall z \in \Sigma^*.\ (xz \in R \Leftrightarrow yz \in R).$$

Example: Let $R = (aa)^* a$

- $a \not\equiv_R aa$? $a\epsilon \in R$ but $aa\epsilon \notin R$ $a \not\equiv_R aa$
- $a \equiv_R aaa$?
- What are the equivalence classes?

$[\epsilon] = (aa)^*$

$[a] = (aa)^* a$

Language Induced Equivalence is also called Nerode Congruence

$R = a^* b^*$

$a \stackrel{?}{\equiv}_R aa$

a^* $\xrightarrow{b}$ $a^* b^+$ $\circlearrowleft b$

$a \cdot a^* \in R \qquad aa \cdot a^* \in R$

$a \cdot a^* b^* \in R \qquad aa \cdot a^* b^* \in R$

$a \cdot a^* b^+ a \Sigma^* \notin R$

REST

$a^* b^+ a \Sigma^*$

$aabbb\underbrace{ax}$

Example

Let $R = \{a^n b^n \mid 0 \leq n\}$. Give equivalence classes of $\equiv_R$.

$\epsilon \overset{?}{\equiv}_R a$ $\qquad \epsilon \not\equiv_R a$

$C_n = \{a^n\}$ $\qquad$ aab Z $\quad$ aaabb Z

$H_k = \{a^m b^n \mid 0 \leq m - n = k\}$ $\qquad$ Z $\epsilon - a \cdot \Sigma^*$

$n > 0$ $\qquad$ Z $\epsilon - b$

REST $\qquad$ Z $\epsilon - bbb^*$

$a^* b^+ a \Sigma^*$ $\qquad$ $aab \equiv_R aaabb$

Properties of Language Induced Equivalence

Recall $x \equiv_R y \stackrel{\text{def}}{=} \forall z \in \Sigma^*. \; (xz \in R \Leftrightarrow yz \in R)$.

.

Recall $x \equiv_R y \stackrel{\text{def}}{=} \forall z \in \Sigma^*. \ (xz \in R \Leftrightarrow yz \in R)$.

Proposition $\equiv_R$ is right congruent.

$x \equiv_R y \Leftrightarrow \forall z. (xz \in R \Leftrightarrow yz \in R)$

$\Rightarrow \forall aw. (\underline{xa}w \in R \Leftrightarrow \underline{ya}w \in R)$

$\Rightarrow xa \equiv_R ya$

Properties of Language Induced Equivalence

Recall $x \equiv_R y \stackrel{\text{def}}{=} \forall z \in \Sigma^*. \ (xz \in R \Leftrightarrow yz \in R)$.

Proposition $\equiv_R$ is right congruent.

Proposition $\equiv_R$ refines R.

$x \equiv_R y \Leftrightarrow \forall z. (xz \in R \Leftrightarrow yz \in R)$

$\Rightarrow (x\epsilon \in R \Leftrightarrow y\epsilon \in R)$

$\therefore \equiv_R$ refines R.

Lemma: If $\equiv$ is right congruence then
$x \equiv y \Rightarrow \forall z.\ xz \equiv yz.$

Recall $x \equiv_R y \stackrel{\text{def}}{=} \forall z \in \Sigma^*.\ (xz \in R \Leftrightarrow yz \in R)$.

Proposition $\equiv_R$ is right congruent.

Proposition $\equiv_R$ refines R.

Proposition(Coarseness) Let $\equiv$ be right-congruent refining R.
Then, $\equiv \ \subseteq \ \equiv_R$.

$x \equiv y \Rightarrow \forall z.\ xz \in R \Longleftrightarrow yz \in R$

$\Rightarrow x \equiv_R y.$

Myhill-Nerode Theorem

Let $R \subseteq \Sigma^*$. The following statements are equivalent.

1. R is regular
2. There exists a Myhill-Nerode relation refining R.
3. The relation $\equiv_R$ is of finite index.

The automaton $A_{\equiv_R}$ gives the minimal DFA for R.

Proof

1) $\Rightarrow$ 2)

1) $\Rightarrow$ DFA M for R

$\Rightarrow$ $\equiv_M$ is Myhill nerode

2) $\Rightarrow$ 3)

2) $\equiv$ is Myhill Nerode for R.

$\therefore$ $\equiv$ of finite index.

$\equiv \;\subseteq\; \equiv_R$

$\therefore$ Index $\equiv\; \geq$ Index $\equiv_R$.

$\therefore$ $\equiv_R$ is of finite index

3) $\Rightarrow$ 1)

$\equiv_R$ is Myhill nerode refining R

$\therefore$ A $\equiv_R$ is FSM accepting R

$\therefore$ R is regular

State Minimization using Quotienting is Optimal

$p \approx_M q \implies p = q$

Let A recognise R. Consider the quotient automaton $M = A/\approx$ as before, and assume that it has no inaccessible states.

Lemma $x \equiv_R y \Leftrightarrow x \equiv_M y$

$x \equiv_R y$ iff $\forall z. (xz \in R \Leftrightarrow yz \in R)$

$\hat{\delta}_M(\hat{\delta}_M(q_0, x), z) \in F) \Longleftrightarrow \hat{\delta}_M(\hat{\delta}_M(q_0, y), z) \in F)$

$\hat{\delta}_M(q_0, x) \approx_M \hat{\delta}_M(q_0, y) \implies \hat{\delta}_M(q_0, x) = \hat{\delta}_M(q_0, y)$

iff $x \equiv_M y$.