Computability and Complexity
COSC 4200

The Myhill-Nerode Theorem

The Relation $\equiv_M$

Let $A \subseteq \Sigma^*$ be a regular language, and let $M = (Q, \Sigma, \delta, q_0, F)$ be a DFA for A with no inaccessible states.

M induces an equivalence relation $\equiv_M$ on Σ^* defined by

$$x \equiv_M y \iff \delta^*(q_0, x) = \delta^*(q_0, y)$$

for all $x, y \in \Sigma^*$.

Properties of $\equiv_M$

Besides the reflexive, symmetric, and transitive properties, $\equiv_M$ satisfies a few other useful properties:

Properties of $\equiv_M$

Besides the reflexive, symmetric, and transitive properties, $\equiv_M$ satisfies a few other useful properties:

1. It is a *right congruence*: for all $x, y \in \Sigma^*$ and $a \in \Sigma$,

$$x \equiv_M y \Longrightarrow xa \equiv_M ya.$$

Properties of $\equiv_M$

Besides the reflexive, symmetric, and transitive properties, $\equiv_M$ satisfies a few other useful properties:

1. It is a *right congruence*: for all $x, y \in \Sigma^*$ and $a \in \Sigma$,

$$x \equiv_M y \Longrightarrow xa \equiv_M ya.$$

2. It *refines* A: for all $x, y \in \Sigma^*$,

$$x \equiv_M y \Longrightarrow \left(x \in A \Leftrightarrow y \in A\right).$$

Properties of $\equiv_M$

Besides the reflexive, symmetric, and transitive properties, $\equiv_M$ satisfies a few other useful properties:

1. It is a *right congruence*: for all $x, y \in \Sigma^*$ and $a \in \Sigma$,

$$x \equiv_M y \implies xa \equiv_M ya.$$

2. It *refines A*: for all $x, y \in \Sigma^*$,

$$x \equiv_M y \implies (x \in A \Leftrightarrow y \in A).$$

3. It is of *finite index*: it has only finitely many equivalence classes.

Myhill-Nerode Relations

Definition. Let $A \subseteq \Sigma^*$. An equivalence relation $\equiv$ on Σ^* is called a *Myhill-Nerode relation* for A if it has the three properties from the previous slide: that is, it is a right congruence of finite index that refines A.

Myhill-Nerode Relations

Definition. Let $A \subseteq \Sigma^*$. An equivalence relation $\equiv$ on Σ^* is called a *Myhill-Nerode relation* for A if it has the three properties from the previous slide: that is, it is a right congruence of finite index that refines A.

- We saw that every DFA M for A yields a Myhill-Nerode relation $\equiv_M$ for A.

Myhill-Nerode Relations

Definition. Let $A \subseteq \Sigma^*$. An equivalence relation $\equiv$ on Σ^* is called a *Myhill-Nerode relation* for A if it has the three properties from the previous slide: that is, it is a right congruence of finite index that refines A.

- We saw that every DFA M for A yields a Myhill-Nerode relation $\equiv_M$ for A.
- We will now show that every Myhill-Nerode relation $\equiv$ for A yields a DFA $M_\equiv$ for A.

From Myhill-Nerode Relation $\equiv$ to the DFA $M_{\equiv}$

Let $A \subseteq \Sigma^*$ and let $\equiv$ be an arbitrary Myhill-Nerode relation for A.

From Myhill-Nerode Relation $\equiv$ to the DFA $M_\equiv$

Let $A \subseteq \Sigma^*$ and let $\equiv$ be an arbitrary Myhill-Nerode relation for A.

The $\equiv$-class of a string $x \in \Sigma^*$ is

$$[x] = \{y \mid y \equiv x\}.$$

From Myhill-Nerode Relation $\equiv$ to the DFA $M_{\equiv}$

Let $A \subseteq \Sigma^*$ and let $\equiv$ be an arbitrary Myhill-Nerode relation for A.

The $\equiv$-class of a string $x \in \Sigma^*$ is

$$[x] = \{y \mid y \equiv x\}.$$

There are finitely many $\equiv$-classes since $\equiv$ has finite index.

From Myhill-Nerode Relation $\equiv$ to the DFA $M_\equiv$

Let $A \subseteq \Sigma^*$ and let $\equiv$ be an arbitrary Myhill-Nerode relation for A.

The $\equiv$-class of a string $x \in \Sigma^*$ is

$$[x] = \{y \mid y \equiv x\}.$$

There are finitely many $\equiv$-classes since $\equiv$ has finite index.

We define the DFA $M_\equiv = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$

From Myhill-Nerode Relation $\equiv$ to the DFA $M_\equiv$

Let $A \subseteq \Sigma^*$ and let $\equiv$ be an arbitrary Myhill-Nerode relation for A.

The $\equiv$-class of a string $x \in \Sigma^*$ is

$$[x] = \{y \mid y \equiv x\}.$$

There are finitely many $\equiv$-classes since $\equiv$ has finite index.

We define the DFA $M_\equiv = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$
- $q_0 = [\epsilon]$

From Myhill-Nerode Relation $\equiv$ to the DFA $M_\equiv$

Let $A \subseteq \Sigma^*$ and let $\equiv$ be an arbitrary Myhill-Nerode relation for A.

The $\equiv$-class of a string $x \in \Sigma^*$ is

$$[x] = \{y \mid y \equiv x\}.$$

There are finitely many $\equiv$-classes since $\equiv$ has finite index.

We define the DFA $M_\equiv = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$
- $q_0 = [\epsilon]$
- $F = \{[x] \mid x \in A\}$

From Myhill-Nerode Relation $\equiv$ to the DFA $M_{\equiv}$

Let $A \subseteq \Sigma^*$ and let $\equiv$ be an arbitrary Myhill-Nerode relation for A.

The $\equiv$-class of a string $x \in \Sigma^*$ is

$$[x] = \{y \mid y \equiv x\}.$$

There are finitely many $\equiv$-classes since $\equiv$ has finite index.

We define the DFA $M_{\equiv} = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$
- $q_0 = [\epsilon]$
- $F = \{[x] \mid x \in A\}$
- $\delta([x], a) = [xa]$ for all $x \in \Sigma^*$ and $a \in \Sigma$

From Myhill-Nerode Relation $\equiv$ to the DFA $M_\equiv$

Let $A \subseteq \Sigma^*$ and let $\equiv$ be an arbitrary Myhill-Nerode relation for A.

The $\equiv$-class of a string $x \in \Sigma^*$ is

$$[x] = \{y \mid y \equiv x\}.$$

There are finitely many $\equiv$-classes since $\equiv$ has finite index.

We define the DFA $M_\equiv = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$
- $q_0 = [\epsilon]$
- $F = \{[x] \mid x \in A\}$
- $\delta([x], a) = [xa]$ for all $x \in \Sigma^*$ and $a \in \Sigma$

Because $\equiv$ is a right congruence, δ is well defined.

From Myhill-Nerode Relation $\equiv$ to the DFA $M_\equiv$

Let $A \subseteq \Sigma^*$ and let $\equiv$ be an arbitrary Myhill-Nerode relation for A.

The $\equiv$-class of a string $x \in \Sigma^*$ is

$$[x] = \{y \mid y \equiv x\}.$$

There are finitely many $\equiv$-classes since $\equiv$ has finite index.

We define the DFA $M_\equiv = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$
- $q_0 = [\epsilon]$
- $F = \{[x] \mid x \in A\}$
- $\delta([x], a) = [xa]$ for all $x \in \Sigma^*$ and $a \in \Sigma$

Because $\equiv$ is a right congruence, δ is well defined.
Since $\equiv$ refines A, we have $x \in A \Leftrightarrow [x] \in F$ for all $x \in \Sigma^*$.

Lemma

For all $x, y \in \Sigma^*$, $\delta^*([x], y) = [xy]$.

Lemma

For all $x, y \in \Sigma^*$, $\delta^*([x], y) = [xy]$.

Proof. By induction on y.

Base case. $y = \epsilon$:

$$\delta^*([x], \epsilon) = [x] = [x\epsilon].$$

Lemma

For all $x, y \in \Sigma^*$, $\delta^*([x], y) = [xy]$.

Proof. By induction on y.

Base case. $y = \epsilon$:

$$\delta^*([x], \epsilon) = [x] = [x\epsilon].$$

Inductive hypothesis. Suppose $\delta^*([x], y) = [xy]$ holds for some string $y \in \Sigma^*$.

Lemma

For all $x, y \in \Sigma^*$, $\delta^*([x], y) = [xy]$.

Proof. By induction on y.

Base case. $y = \epsilon$:

$$\delta^*([x], \epsilon) = [x] = [x\epsilon].$$

Inductive hypothesis. Suppose $\delta^*([x], y) = [xy]$ holds for some string $y \in \Sigma^*$.

Inductive step. We must show $\delta^*([x], ya) = [xya]$ for all $a \in \Sigma$.

$$\delta^*([x], ya)$$

Lemma

For all $x, y \in \Sigma^*$, $\delta^*([x], y) = [xy]$.

Proof. By induction on y.

Base case. $y = \epsilon$:

$$\delta^*([x], \epsilon) = [x] = [x\epsilon].$$

Inductive hypothesis. Suppose $\delta^*([x], y) = [xy]$ holds for some string $y \in \Sigma^*$.

Inductive step. We must show $\delta^*([x], ya) = [xya]$ for all $a \in \Sigma$.

$$\delta^*([x], ya) \quad = \quad \delta(\delta^*([x], y), a) \quad \text{definition of } \delta^*$$

Lemma

For all $x, y \in \Sigma^*$, $\delta^*([x], y) = [xy]$.

Proof. By induction on y.

Base case. $y = \epsilon$:

$$\delta^*([x], \epsilon) = [x] = [x\epsilon].$$

Inductive hypothesis. Suppose $\delta^*([x], y) = [xy]$ holds for some string $y \in \Sigma^*$.

Inductive step. We must show $\delta^*([x], ya) = [xya]$ for all $a \in \Sigma$.

$$\begin{array}{rcll} \delta^*([x], ya) & = & \delta(\delta^*([x], y), a) & \text{definition of } \delta^* \\ & = & \delta([xy], a) & \text{inductive hypothesis} \end{array}$$

Lemma

For all $x, y \in \Sigma^*$, $\delta^*([x], y) = [xy]$.

Proof. By induction on y.

Base case. $y = \epsilon$:

$$\delta^*([x], \epsilon) = [x] = [x\epsilon].$$

Inductive hypothesis. Suppose $\delta^*([x], y) = [xy]$ holds for some string $y \in \Sigma^*$.

Inductive step. We must show $\delta^*([x], ya) = [xya]$ for all $a \in \Sigma$.

$$\begin{array}{rcll} \delta^*([x], ya) & = & \delta(\delta^*([x], y), a) & \text{definition of } \delta^* \\ & = & \delta([xy], a) & \text{inductive hypothesis} \\ & = & [xya] & \text{definition of } \delta \end{array}$$

$\square$

Recall $\equiv$ is a Myhill-Nerode relation for A and $M_{\equiv} = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$
- $q_0 = [\epsilon]$
- $F = \{[x] \mid x \in A\}$
- $\delta([x], a) = [xa]$ for all $x \in \Sigma^*$ and $a \in \Sigma$

Theorem

$L(M_{\equiv}) = A$.

Recall $\equiv$ is a Myhill-Nerode relation for A and $M_\equiv = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$
- $q_0 = [\epsilon]$
- $F = \{[x] \mid x \in A\}$
- $\delta([x], a) = [xa]$ for all $x \in \Sigma^*$ and $a \in \Sigma$

Theorem

$L(M_\equiv) = A$.

Proof. For any $x \in \Sigma^*$,

$$x \in L(M_\equiv) \iff \delta^*([\epsilon], x) \in F \quad \text{definition of acceptance}$$

Recall $\equiv$ is a Myhill-Nerode relation for A and $M_{\equiv} = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$
- $q_0 = [\epsilon]$
- $F = \{[x] \mid x \in A\}$
- $\delta([x], a) = [xa]$ for all $x \in \Sigma^*$ and $a \in \Sigma$

Theorem

$L(M_{\equiv}) = A$.

Proof. For any $x \in \Sigma^*$,

$$\begin{array}{rcll} x \in L(M_{\equiv}) & \Longleftrightarrow & \delta^*([\epsilon], x) \in F & \text{definition of acceptance} \\ & \Longleftrightarrow & [x] \in F & \text{Lemma} \end{array}$$

Recall $\equiv$ is a Myhill-Nerode relation for A and $M_{\equiv} = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$
- $q_0 = [\epsilon]$
- $F = \{[x] \mid x \in A\}$
- $\delta([x], a) = [xa]$ for all $x \in \Sigma^*$ and $a \in \Sigma$

Theorem

$L(M_{\equiv}) = A$.

Proof. For any $x \in \Sigma^*$,

$$\begin{array}{rcll} x \in L(M_{\equiv}) & \iff & \delta^*([\epsilon], x) \in F & \text{definition of acceptance} \\ & \iff & [x] \in F & \text{Lemma} \\ & \iff & x \in A & \equiv \text{ refines } A \end{array}$$

Recall $\equiv$ is a Myhill-Nerode relation for A and $M_{\equiv} = (Q, \Sigma, \delta, q_0, F)$ where

- $Q = \{[x] \mid x \in \Sigma^*\}$
- $q_0 = [\epsilon]$
- $F = \{[x] \mid x \in A\}$
- $\delta([x], a) = [xa]$ for all $x \in \Sigma^*$ and $a \in \Sigma$

Theorem

$L(M_{\equiv}) = A$.

Proof. For any $x \in \Sigma^*$,

$$\begin{array}{rcll} x \in L(M_{\equiv}) & \Longleftrightarrow & \delta^*([\epsilon], x) \in F & \text{definition of acceptance} \\ & \Longleftrightarrow & [x] \in F & \text{Lemma} \\ & \Longleftrightarrow & x \in A & \equiv \ \text{refines } A \end{array}$$

Therefore $L(M_{\equiv}) = A$. $\square$

The following lemma states the mappings $M \to \equiv_M$ and $\equiv \to M_\equiv$ are inverses of each other, up to isomorphism of automaton.

Lemma

The following lemma states the mappings $M \to \equiv_M$ and $\equiv \to M_\equiv$ are inverses of each other, up to isomorphism of automaton.

Lemma

1. *If $\equiv$ is a Myhill-Nerode relation for A, and if we apply the construction $\equiv \to M_\equiv$ and then apply the construction $M_\equiv \to \equiv_{M_\equiv}$, the relation $\equiv_{M_\equiv}$ is identical to $\equiv$.*

$$\equiv \to M_\equiv \to \equiv_{M_\equiv} = \equiv$$

The following lemma states the mappings $M \rightarrow \equiv_M$ and $\equiv \rightarrow M_\equiv$ are inverses of each other, up to isomorphism of automaton.

Lemma

1. *If $\equiv$ is a Myhill-Nerode relation for A, and if we apply the construction $\equiv \rightarrow M_\equiv$ and then apply the construction $M_\equiv \rightarrow \equiv_{M_\equiv}$, the relation $\equiv_{M_\equiv}$ is identical to $\equiv$.*

$$\equiv \; \rightarrow M_\equiv \rightarrow \; \equiv_{M_\equiv} \; = \; \equiv$$

2. *If M is a DFA for A with no inaccessible states, and if we apply the construction $M \rightarrow \equiv_M$ and then apply the construction $\equiv_M \rightarrow M_{\equiv_M}$, the resulting DFA $M_{\equiv_M}$ is isomorphic to M.*

$$M \rightarrow \; \equiv_M \; \rightarrow M_{\equiv_M} \cong M$$

Refining Relations

A relation $\equiv_1$ *refines* a relation $\equiv_2$ if

$$x \equiv_1 y \Rightarrow x \equiv_2 y.$$

Refining Relations

A relation $\equiv_1$ *refines* a relation $\equiv_2$ if

$$x \equiv_1 y \Rightarrow x \equiv_2 y.$$

- If $\equiv_1$ and $\equiv_2$ are equivalence relations, this says that all of $\equiv_1$'s equivalence classes are contained in equivalence classes of $\equiv_2$.

Refining Relations

A relation $\equiv_1$ *refines* a relation $\equiv_2$ if

$$x \equiv_1 y \Rightarrow x \equiv_2 y.$$

- If $\equiv_1$ and $\equiv_2$ are equivalence relations, this says that all of $\equiv_1$'s equivalence classes are contained in equivalence classes of $\equiv_2$.
- If $\equiv_1$ refines $\equiv_2$, then we say $\equiv_2$ is *coarser* than $\equiv_1$.

Let $A \subseteq \Sigma^*$. We define an equivalence relation $\equiv_A$ on Σ^* by

$$x \equiv_A y \iff (\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$$

for all $x, y \in \Sigma^*$.

Lemma

Let $A \subseteq \Sigma^*$ The relation $\equiv_A$ is a right congruence refining A and is the coarsest such relation on Σ^*.

Lemma

Let $A \subseteq \Sigma^*$ The relation $\equiv_A$ is a right congruence refining A and is the coarsest such relation on Σ^*.

Proof. For any $x, y \in \Sigma^*$, we have

$$x \equiv_A y \quad \Rightarrow \quad (\forall z \in \Sigma^*)\, (xz \in A \Leftrightarrow yz \in A)$$

Lemma

Let $A \subseteq \Sigma^*$ The relation $\equiv_A$ is a right congruence refining A and is the coarsest such relation on Σ^*.

Proof. For any $x, y \in \Sigma^*$, we have

$$
\begin{aligned}
x \equiv_A y \quad &\Rightarrow \quad (\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A) \\
&\Rightarrow \quad (\forall a \in \Sigma)\ (\forall w \in \Sigma^*)\ (xaw \in A \Leftrightarrow yaw \in A)
\end{aligned}
$$

Lemma

Let $A \subseteq \Sigma^*$ The relation $\equiv_A$ is a right congruence refining A and is the coarsest such relation on Σ^*.

Proof. For any $x, y \in \Sigma^*$, we have

$$\begin{aligned} x \equiv_A y \quad &\Rightarrow \quad (\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A) \\ &\Rightarrow \quad (\forall a \in \Sigma)\ (\forall w \in \Sigma^*)\ (xaw \in A \Leftrightarrow yaw \in A) \\ &\Rightarrow \quad (\forall a \in \Sigma)\ xa \equiv_A ya, \end{aligned}$$

so $\equiv_A$ is a right congruence.

Lemma

Let $A \subseteq \Sigma^*$ The relation $\equiv_A$ is a right congruence refining A and is the coarsest such relation on Σ^*.

Proof. For any $x, y \in \Sigma^*$, we have

$$\begin{aligned} x \equiv_A y &\Rightarrow (\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A) \\ &\Rightarrow (\forall a \in \Sigma)\ (\forall w \in \Sigma^*)\ (xaw \in A \Leftrightarrow yaw \in A) \\ &\Rightarrow (\forall a \in \Sigma)\ xa \equiv_A ya, \end{aligned}$$

so $\equiv_A$ is a right congruence.

To see that $\equiv_A$ refines A, use $z = \epsilon$ in the definition of $\equiv_A$:

$$x \equiv_A y \Rightarrow (x \in A \Leftrightarrow y \in A).$$

Lemma

Let $A \subseteq \Sigma^*$ The relation $\equiv_A$ is a right congruence refining A and is the coarsest such relation on Σ^*.

Proof continued. Let $\equiv$ be any equivalence relation on Σ^* that is a right congruence refining A. We have

$$x \equiv y \quad \Rightarrow \quad (\forall z)\ xz \equiv yz \qquad (\equiv \text{ is a right congruence})$$

Lemma

Let $A \subseteq \Sigma^*$ The relation $\equiv_A$ is a right congruence refining A and is the coarsest such relation on Σ^*.

Proof continued. Let $\equiv$ be any equivalence relation on Σ^* that is a right congruence refining A. We have

$$\begin{array}{lcll} x \equiv y & \Rightarrow & (\forall z)\ xz \equiv yz & (\equiv \text{ is a right congruence}) \\ & \Rightarrow & (\forall z)\ (xz \in A \Leftrightarrow yz \in A) & (\equiv \text{ refines } A) \end{array}$$

Lemma

Let $A \subseteq \Sigma^*$ The relation $\equiv_A$ is a right congruence refining A and is the coarsest such relation on Σ^*.

Proof continued. Let $\equiv$ be any equivalence relation on Σ^* that is a right congruence refining A. We have

$$\begin{aligned} x \equiv y \quad &\Rightarrow \quad (\forall z)\ xz \equiv yz && (\equiv \text{ is a right congruence}) \\ &\Rightarrow \quad (\forall z)\ (xz \in A \Leftrightarrow yz \in A) && (\equiv \text{ refines } A) \\ &\Rightarrow \quad x \equiv_A y, && (\text{definition of } \equiv_A) \end{aligned}$$

so $\equiv_A$ is coarser than $\equiv$. $\square$

Myhill-Nerode Theorem

Let $A \subseteq \Sigma^*$. The following are equivalent:

1. A is regular.
2. There exists a Myhill-Nerode relation for A.
3. The relation $\equiv_A$ is of finite index.

Myhill-Nerode Theorem

Let $A \subseteq \Sigma^*$. The following are equivalent:

1. A is regular.
2. There exists a Myhill-Nerode relation for A.
3. The relation $\equiv_A$ is of finite index.

Proof. 1 $\Rightarrow$ 2: Given a DFA M for A, the construction $M \rightarrow \equiv_M$ yields a Myhill-Nerode relation for A.

Myhill-Nerode Theorem

Let $A \subseteq \Sigma^*$. The following are equivalent:

1. A is regular.
2. There exists a Myhill-Nerode relation for A.
3. The relation $\equiv_A$ is of finite index.

Proof. 1 $\Rightarrow$ 2: Given a DFA M for A, the construction $M \to \equiv_M$ yields a Myhill-Nerode relation for A.

2 $\Rightarrow$ 3: Let $\equiv$ be a Myhill-Nerode relation for A. Then $\equiv$ is a right congruence that refines A, so $\equiv_A$ is coarser than $\equiv$ by the Lemma. Since $\equiv$ is of finite index, this implies $\equiv_A$ is also of finite index.

Myhill-Nerode Theorem

Let $A \subseteq \Sigma^*$. The following are equivalent:

1. A is regular.
2. There exists a Myhill-Nerode relation for A.
3. The relation $\equiv_A$ is of finite index.

Proof. 1 $\Rightarrow$ 2: Given a DFA M for A, the construction $M \to \equiv_M$ yields a Myhill-Nerode relation for A.

2 $\Rightarrow$ 3: Let $\equiv$ be a Myhill-Nerode relation for A. Then $\equiv$ is a right congruence that refines A, so $\equiv_A$ is coarser than $\equiv$ by the Lemma. Since $\equiv$ is of finite index, this implies $\equiv_A$ is also of finite index.

3 $\Rightarrow$ 1: If $\equiv_A$ is of finite index, then it is a Myhill-Nerode relation for A by the Lemma. The construction $\equiv_A \to M_{\equiv_A}$ produces a DFA for A. $\square$

Corollary

For any regular language A, the DFA $M_{\equiv_A}$ is the minimal DFA for A.

Proof. If A is regular, then $\equiv_A$ is a Myhill-Nerode relation for A. Also, it is the coarsest such relation: it has the fewest equivalence classes of any Myhill-Nerode relation for A. Therefore $M_{\equiv_A}$ has the fewest states in a DFA for A. $\square$

Applications

We can use the Myhill-Nerode theorem to prove nonregularity.

Example. $A = \{0^n 1^n \mid n \geq 0\}$ is not regular.

Applications

We can use the Myhill-Nerode theorem to prove nonregularity.

Example. $A = \{0^n 1^n \mid n \geq 0\}$ is not regular.

Proof. If $k \neq m$, then $0^k \not\equiv_A 0^m$ since

$$0^k 1^k \in A \text{ and } 0^m 1^k \notin A.$$

Applications

We can use the Myhill-Nerode theorem to prove nonregularity.

Example. $A = \{0^n 1^n \mid n \geq 0\}$ is not regular.

Proof. If $k \neq m$, then $0^k \not\equiv_A 0^m$ since

$$0^k 1^k \in A \text{ and } 0^m 1^k \notin A.$$

Therefore $\equiv_A$ has infinitely many equivalence classes, at least one for each 0^k, $k \geq 0$. By the Myhill-Nerode Theorem, A is not regular. $\square$

Applications

Example. $B = \{0^{n^2} \mid n \geq 0\}$ is not regular.

Applications

Example. $B = \{0^{n^2} \mid n \geq 0\}$ is not regular.

Proof. For any $0 \leq k < j$, $0^{k^2} \not\equiv_B 0^{j^2}$ since

$$0^{k^2} 0^{2k+1} \in B \text{ and } 0^{j^2} 0^{2k+1} \notin B.$$

- $0^{k^2} 0^{2k+1} \in B$ because $k^2 + 2k + 1 = (k+1)^2$.

Applications

Example. $B = \{0^{n^2} \mid n \geq 0\}$ is not regular.

Proof. For any $0 \leq k < j$, $0^{k^2} \not\equiv_B 0^{j^2}$ since

$$0^{k^2}0^{2k+1} \in B \text{ and } 0^{j^2}0^{2k+1} \notin B.$$

- $0^{k^2}0^{2k+1} \in B$ because $k^2 + 2k + 1 = (k+1)^2$.
- $0^{j^2}0^{2k+1} \notin B$ because $j^2 < j^2 + 2k + 1 < j^2 + 2j + 1 = (j+1)^2$ implies $j^2 + 2k + 1$ is not a square.

Applications

Example. $B = \{0^{n^2} \mid n \geq 0\}$ is not regular.

Proof. For any $0 \leq k < j$, $0^{k^2} \not\equiv_B 0^{j^2}$ since

$$0^{k^2}0^{2k+1} \in B \text{ and } 0^{j^2}0^{2k+1} \notin B.$$

- $0^{k^2}0^{2k+1} \in B$ because $k^2 + 2k + 1 = (k+1)^2$.
- $0^{j^2}0^{2k+1} \notin B$ because $j^2 < j^2 + 2k + 1 < j^2 + 2j + 1 = (j+1)^2$ implies $j^2 + 2k + 1$ is not a square.

Therefore $\equiv_B$ has infinitely many equivalence classes, so B is not regular by the Myhill-Nerode Theorem. $\square$

Applications

Example. $F = \{a^m b^n c^l \mid m, n, l \geq 0 \text{ and if } m = 1 \text{ then } n = l\}$

Recall that we showed F satisfies the conclusion of the Pumping Lemma. We can use the Myhill-Nerode Theorem to prove F is not regular.

Applications

Example. $F = \{a^m b^n c^l \mid m, n, l \geq 0 \text{ and if } m = 1 \text{ then } n = l\}$

Recall that we showed F satisfies the conclusion of the Pumping Lemma. We can use the Myhill-Nerode Theorem to prove F is not regular.

Proof. For all $i < j$, $ab^i \not\equiv_F ab^j$ since

$$ab^i c^i \in A \text{ and } ab^j c^i \notin F.$$

Therefore $\equiv_F$ has infinitely many equivalence classes, so F is not regular by the Myhill-Nerode Theorem. $\square$

Let A be a regular language and let $M = (Q, \Sigma, \delta, q_0, F)$ be the minimal DFA for A.

Recall that for every $x, y \in \Sigma^*$,

$$x \equiv_A y \text{ if } (\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$$

and

$$x \equiv_M y \text{ if } \delta^*(q_0, x) = \delta^*(q_0, y).$$

Let A be a regular language and let $M = (Q, \Sigma, \delta, q_0, F)$ be the minimal DFA for A.

Recall that for every $x, y \in \Sigma^*$,

$$x \equiv_A y \text{ if } (\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$$

and

$$x \equiv_M y \text{ if } \delta^*(q_0, x) = \delta^*(q_0, y).$$

From the proof of the Myhill-Nerode Theorem, we know that $\equiv_A$ and $\equiv_M$ are the same relation. In other words, the states of M "remember" the equivalence of x with respect to $\equiv_A$:

$$\delta^*(q_0, x) \text{ is essentially } [x]_A.$$

Let $A = \{x00 \mid x \in \{0,1\}^*\}$.
Recall $x \equiv_A y$ if $(\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$.

1. What is $\equiv_A$-equivalent to ϵ?

Let $A = \{x00 \mid x \in \{0,1\}^*\}$.
Recall $x \equiv_A y$ if $(\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$.

1. What is $\equiv_A$-equivalent to ϵ?
    - $\epsilon \equiv_A 1 \quad \epsilon \equiv_A 11 \quad \epsilon \equiv_A 01$

Let $A = \{x00 \mid x \in \{0,1\}^*\}$.

Recall $x \equiv_A y$ if $(\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$.

1. What is $\equiv_A$-equivalent to ϵ?
    - $\epsilon \equiv_A 1 \quad \epsilon \equiv_A 11 \quad \epsilon \equiv_A 01$
    - $\epsilon \not\equiv_A 0$ ($\epsilon 0 \notin A$ but $00 \in A$)
    - $\epsilon \not\equiv_A 00$ ($\epsilon \notin A$ but $00 \in A$)

Let $A = \{x00 \mid x \in \{0,1\}^*\}$.

Recall $x \equiv_A y$ if $(\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$.

1. What is $\equiv_A$-equivalent to ϵ?
   - $\epsilon \equiv_A 1 \quad \epsilon \equiv_A 11 \quad \epsilon \equiv_A 01$
   - $\epsilon \not\equiv_A 0$ ($\epsilon 0 \notin A$ but $00 \in A$)
   - $\epsilon \not\equiv_A 00$ ($\epsilon \notin A$ but $00 \in A$)

$$\begin{aligned} [\epsilon]_A &= \{\epsilon\} \cup \{x \in \{0,1\}^* \mid x \text{ ends in } 1\} \\ &= \{x \in \{0,1\}^* \mid x \text{ does not end in } 0\} \end{aligned}$$

Let $A = \{x00 \mid x \in \{0,1\}^*\}$.
Recall $x \equiv_A y$ if $(\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$.

1. What is $\equiv_A$-equivalent to ϵ?
   - $\epsilon \equiv_A 1 \quad \epsilon \equiv_A 11 \quad \epsilon \equiv_A 01$
   - $\epsilon \not\equiv_A 0$ ($\epsilon 0 \notin A$ but $00 \in A$)
   - $\epsilon \not\equiv_A 00$ ($\epsilon \notin A$ but $00 \in A$)

$$\begin{aligned} [\epsilon]_A &= \{\epsilon\} \cup \{x \in \{0,1\}^* \mid x \text{ ends in } 1\} \\ &= \{x \in \{0,1\}^* \mid x \text{ does not end in } 0\} \end{aligned}$$

2. What is $\equiv_A$-equivalent to 0?
   - $0 \equiv_A 10 \quad 0 \equiv_A 1010 \quad 0 \equiv_A 0010$

Let $A = \{x00 \mid x \in \{0,1\}^*\}$.

Recall $x \equiv_A y$ if $(\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$.

1. What is $\equiv_A$-equivalent to ϵ?
   - $\epsilon \equiv_A 1 \quad \epsilon \equiv_A 11 \quad \epsilon \equiv_A 01$
   - $\epsilon \not\equiv_A 0$ ($\epsilon 0 \notin A$ but $00 \in A$)
   - $\epsilon \not\equiv_A 00$ ($\epsilon \notin A$ but $00 \in A$)

$$\begin{aligned}[\epsilon]_A &= \{\epsilon\} \cup \{x \in \{0,1\}^* \mid x \text{ ends in } 1\} \\ &= \{x \in \{0,1\}^* \mid x \text{ does not end in } 0\}\end{aligned}$$

2. What is $\equiv_A$-equivalent to 0?
   - $0 \equiv_A 10 \quad 0 \equiv_A 1010 \quad 0 \equiv_A 0010$
   - $0 \not\equiv_A 100$ ($0 \notin A$ but $100 \in A$)
   - $0 \not\equiv_A 1$ ($00 \in A$ but $10 \notin A$)

$$[0]_A = \{x \in \{0,1\}^* \mid x \text{ ends in exactly one } 0\}$$

Let $A = \{x00 \mid x \in \{0,1\}^*\}$.
Recall $x \equiv_A y$ if $(\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$.

1. What is $\equiv_A$-equivalent to ϵ?
   - $\epsilon \equiv_A 1 \quad \epsilon \equiv_A 11 \quad \epsilon \equiv_A 01$
   - $\epsilon \not\equiv_A 0$ ($\epsilon 0 \notin A$ but $00 \in A$)
   - $\epsilon \not\equiv_A 00$ ($\epsilon \notin A$ but $00 \in A$)

$$\begin{aligned} [\epsilon]_A &= \{\epsilon\} \cup \{x \in \{0,1\}^* \mid x \text{ ends in } 1\} \\ &= \{x \in \{0,1\}^* \mid x \text{ does not end in } 0\} \end{aligned}$$

2. What is $\equiv_A$-equivalent to 0?
   - $0 \equiv_A 10 \quad 0 \equiv_A 1010 \quad 0 \equiv_A 0010$
   - $0 \not\equiv_A 100$ ($0 \notin A$ but $100 \in A$)
   - $0 \not\equiv_A 1$ ($00 \in A$ but $10 \notin A$)

$$[0]_A = \{x \in \{0,1\}^* \mid x \text{ ends in exactly one } 0\}$$

3. What is $\equiv_A$-equivalent to 00?
   - $00 \equiv_A 100 \quad 00 \equiv_A 10100 \quad 00 \equiv_A 10000$

Let $A = \{x00 \mid x \in \{0,1\}^*\}$.
Recall $x \equiv_A y$ if $(\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$.

1. What is $\equiv_A$-equivalent to ϵ?
   - $\epsilon \equiv_A 1 \quad \epsilon \equiv_A 11 \quad \epsilon \equiv_A 01$
   - $\epsilon \not\equiv_A 0$ ($\epsilon 0 \notin A$ but $00 \in A$)
   - $\epsilon \not\equiv_A 00$ ($\epsilon \notin A$ but $00 \in A$)

$$\begin{aligned} [\epsilon]_A &= \{\epsilon\} \cup \{x \in \{0,1\}^* \mid x \text{ ends in } 1\} \\ &= \{x \in \{0,1\}^* \mid x \text{ does not end in } 0\} \end{aligned}$$

2. What is $\equiv_A$-equivalent to 0?
   - $0 \equiv_A 10 \quad 0 \equiv_A 1010 \quad 0 \equiv_A 0010$
   - $0 \not\equiv_A 100$ ($0 \notin A$ but $100 \in A$)
   - $0 \not\equiv_A 1$ ($00 \in A$ but $10 \notin A$)

$$[0]_A = \{x \in \{0,1\}^* \mid x \text{ ends in exactly one } 0\}$$

3. What is $\equiv_A$-equivalent to 00?
   - $00 \equiv_A 100 \quad 00 \equiv_A 10100 \quad 00 \equiv_A 10000$
   - $00 \not\equiv_A 10$ ($00 \in A$ but $10 \notin A$)
   - $00 \not\equiv_A 001$ ($00 \in A$ but $001 \notin A$)

Let $A = \{x00 \mid x \in \{0,1\}^*\}$.
Recall $x \equiv_A y$ if $(\forall z \in \Sigma^*)\ (xz \in A \Leftrightarrow yz \in A)$.

1. What is $\equiv_A$-equivalent to ϵ?
   - $\epsilon \equiv_A 1 \qquad \epsilon \equiv_A 11 \qquad \epsilon \equiv_A 01$
   - $\epsilon \not\equiv_A 0$ ($\epsilon 0 \notin A$ but $00 \in A$)
   - $\epsilon \not\equiv_A 00$ ($\epsilon \notin A$ but $00 \in A$)

$$\begin{aligned} [\epsilon]_A &= \{\epsilon\} \cup \{x \in \{0,1\}^* \mid x \text{ ends in } 1\} \\ &= \{x \in \{0,1\}^* \mid x \text{ does not end in } 0\} \end{aligned}$$

2. What is $\equiv_A$-equivalent to 0?
   - $0 \equiv_A 10 \qquad 0 \equiv_A 1010 \qquad 0 \equiv_A 0010$
   - $0 \not\equiv_A 100$ ($0 \notin A$ but $100 \in A$)
   - $0 \not\equiv_A 1$ ($00 \in A$ but $10 \notin A$)

$$[0]_A = \{x \in \{0,1\}^* \mid x \text{ ends in exactly one } 0\}$$

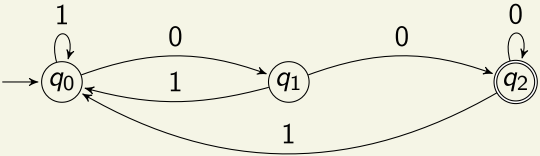
3. What is $\equiv_A$-equivalent to 00?
   - $00 \equiv_A 100 \qquad 00 \equiv_A 10100 \qquad 00 \equiv_A 10000$
   - $00 \not\equiv_A 10$ ($00 \in A$ but $10 \notin A$)
   - $00 \not\equiv_A 001$ ($00 \in A$ but $001 \notin A$)

$$[00]_A = \{x \in \{0,1\}^* \mid x \text{ ends in two or more 0's}\}$$

Example

$$A = \{x00 \mid x \in \{0,1\}^*\}$$

M :



Equivalence classes for $\equiv_M$ and $\equiv_A$:

$[\epsilon]_M =$	$\{x \mid \delta^*(q_0, x) = q_0\} = \epsilon \cup (0 \cup 1)^*1$	$=$	$\left\{ x \;\middle|\; \begin{array}{c} x \text{ does not} \\ \text{end in } 0 \end{array} \right\}$	$= [\epsilon]_A$
$[0]_M =$	$\{x \mid \delta^*(q_0, x) = q_1\} = 0 \cup (0 \cup 1)^*10$	$=$	$\left\{ x \;\middle|\; \begin{array}{c} x \text{ ends in} \\ \text{exactly one } 0 \end{array} \right\}$	$= [0]_A$
$[00]_M =$	$\{x \mid \delta^*(q_0, x) = q_2\} = (0 \cup 1)^*00$	$=$	$\left\{ x \;\middle|\; \begin{array}{c} x \text{ ends in at} \\ \text{least two } 0\text{'s} \end{array} \right\}$	$= [00]_A$

$A = [00]_A$ and $A^c = [\epsilon]_A \cup [0]_A$