6.5
Myhill-Nerode Theorem

One automata to rule them all

"Myhill-Nerode Theorem": A regular language L has a unique (up to naming) minimal automata, and it can be computed efficiently once any DFA is given for L.

6.5.1

Myhill-Nerode Theorem: Equivalence between strings

Indistinguishability

Recall:

Definition

For a language L over Σ and two strings $x, y \in \Sigma^*$ we say that x and y are distinguishable with respect to L if there is a string $w \in \Sigma^*$ such that exactly one of xw, yw is in L. x, y are indistinguishable with respect to L if there is no such w.

Given language L over Σ define a relation $\equiv_L$ over strings in Σ^* as follows: $x \equiv_L y$ iff x and y are indistinguishable with respect to L.

Definition

$x \equiv_L y$ *means that* $\forall w \in \Sigma^*$: $xw \in L \iff yw \in L$.
In words: x *is equivalent to* y *under* L.

Indistinguishability

Recall:

Definition

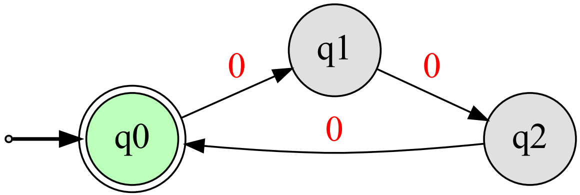
For a language L over Σ and two strings $x, y \in \Sigma^*$ we say that x and y are distinguishable with respect to L if there is a string $w \in \Sigma^*$ such that exactly one of xw, yw is in L. x, y are indistinguishable with respect to L if there is no such w.

Given language L over Σ define a relation $\equiv_L$ over strings in Σ^* as follows: $x \equiv_L y$ iff x and y are indistinguishable with respect to L.

Definition

$x \equiv_L y$ means that $\forall w \in \Sigma^*$: $xw \in L \iff yw \in L$.
In words: x is equivalent to y under L.

Example: Equivalence classes



Indistinguishability

Claim

$\equiv_L$ is an equivalence relation over Σ^*.

Proof.

1. Reflexive: $\forall x \in \Sigma^*: \forall w \in \Sigma^*: xw \in L \iff xw \in L. \implies x \equiv_L x.$
2. Symmetry: $x \equiv_L y$ then $\forall w \in \Sigma^*: xw \in L \iff yw \in L$
   $\forall w \in \Sigma^*: yw \in L \iff xw \in L \implies y \equiv_L x$.
3. Transitivity: $x \equiv_L y$ and $y \equiv_L z$
   $\forall w \in \Sigma^*: xw \in L \iff yw \in L$ and $\forall w \in \Sigma^*: yw \in L \iff zw \in L$
   $\implies \forall w \in \Sigma^*: xw \in L \iff zw \in L$
   $\implies x \equiv_L z.$

Indistinguishability

Claim

$\equiv_L$ *is an equivalence relation over* Σ^*.

Proof.

1. Reflexive: $\forall x \in \Sigma^*: \forall w \in \Sigma^*: xw \in L \iff xw \in L. \implies x \equiv_L x$.
2. Symmetry: $x \equiv_L y$ then $\forall w \in \Sigma^*: xw \in L \iff yw \in L$
   $\forall w \in \Sigma^*: yw \in L \iff xw \in L \implies y \equiv_L x$.
3. Transitivity: $x \equiv_L y$ and $y \equiv_L z$
   $\forall w \in \Sigma^*: xw \in L \iff yw \in L$ and $\forall w \in \Sigma^*: yw \in L \iff zw \in L$
   $\implies \forall w \in \Sigma^*: xw \in L \iff zw \in L$
   $\implies x \equiv_L z$.

□

Indistinguishability

Claim

$\equiv_L$ *is an equivalence relation over* Σ^*.

Proof.

1. Reflexive: $\forall x \in \Sigma^*$: $\forall w \in \Sigma^*$: $xw \in L \iff xw \in L. \implies x \equiv_L x$.
2. Symmetry: $x \equiv_L y$ then $\forall w \in \Sigma^*$: $xw \in L \iff yw \in L$
   $\forall w \in \Sigma^*$: $yw \in L \iff xw \in L \implies y \equiv_L x$.
3. Transitivity: $x \equiv_L y$ and $y \equiv_L z$
   $\forall w \in \Sigma^*$: $xw \in L \iff yw \in L$ and $\forall w \in \Sigma^*$: $yw \in L \iff zw \in L$
   $\implies \forall w \in \Sigma^*$: $xw \in L \iff zw \in L$
   $\implies x \equiv_L z$.

□

Indistinguishability

Claim

$\equiv_L$ is an equivalence relation over Σ^*.

Proof.

1. Reflexive: $\forall x \in \Sigma^*$: $\forall w \in \Sigma^*$: $xw \in L \iff xw \in L$. $\implies x \equiv_L x$.
2. Symmetry: $x \equiv_L y$ then $\forall w \in \Sigma^*$: $xw \in L \iff yw \in L$
   $\forall w \in \Sigma^*$: $yw \in L \iff xw \in L \implies y \equiv_L x$.
3. Transitivity: $x \equiv_L y$ and $y \equiv_L z$
   $\forall w \in \Sigma^*$: $xw \in L \iff yw \in L$ and $\forall w \in \Sigma^*$: $yw \in L \iff zw \in L$
   $\implies \forall w \in \Sigma^*$: $xw \in L \iff zw \in L$
   $\implies x \equiv_L z$.

□

Indistinguishability

Claim

$\equiv_L$ is an equivalence relation over Σ^*.

Proof.

1. Reflexive: $\forall x \in \Sigma^*: \forall w \in \Sigma^*: xw \in L \iff xw \in L. \implies x \equiv_L x.$
2. Symmetry: $x \equiv_L y$ then $\forall w \in \Sigma^*: xw \in L \iff yw \in L$
   $\forall w \in \Sigma^*: yw \in L \iff xw \in L \implies y \equiv_L x$.
3. Transitivity: $x \equiv_L y$ and $y \equiv_L z$
   $\forall w \in \Sigma^*: xw \in L \iff yw \in L$ and $\forall w \in \Sigma^*: yw \in L \iff zw \in L$
   $\implies \forall w \in \Sigma^*: xw \in L \iff zw \in L$
   $\implies x \equiv_L z$.

Indistinguishability

Claim

$\equiv_L$ *is an equivalence relation over* Σ^*.

Proof.

1. Reflexive: $\forall x \in \Sigma^*$: $\forall w \in \Sigma^*$: $xw \in L \iff xw \in L$. $\implies x \equiv_L x$.
2. Symmetry: $x \equiv_L y$ then $\forall w \in \Sigma^*$: $xw \in L \iff yw \in L$
   $\forall w \in \Sigma^*$: $yw \in L \iff xw \in L \implies y \equiv_L x$.
3. Transitivity: $x \equiv_L y$ and $y \equiv_L z$
   $\forall w \in \Sigma^*$: $xw \in L \iff yw \in L$ and $\forall w \in \Sigma^*$: $yw \in L \iff zw \in L$
   $\implies \forall w \in \Sigma^*$: $xw \in L \iff zw \in L$
   $\implies x \equiv_L z$.

Indistinguishability

Claim

$\equiv_L$ is an equivalence relation over Σ^*.

Proof.

1. Reflexive: $\forall x \in \Sigma^*$: $\forall w \in \Sigma^*$: $xw \in L \iff xw \in L$. $\implies x \equiv_L x$.
2. Symmetry: $x \equiv_L y$ then $\forall w \in \Sigma^*$: $xw \in L \iff yw \in L$
   $\forall w \in \Sigma^*$: $yw \in L \iff xw \in L \implies y \equiv_L x$.
3. Transitivity: $x \equiv_L y$ and $y \equiv_L z$
   $\forall w \in \Sigma^*$: $xw \in L \iff yw \in L$ and $\forall w \in \Sigma^*$: $yw \in L \iff zw \in L$
   $\implies \forall w \in \Sigma^*$: $xw \in L \iff zw \in L$
   $\implies x \equiv_L z$.

□

Equivalences over automatas...

Claim (Just proved.)

$\equiv_L$ *is an equivalence relation over* Σ^*.

Therefore, $\equiv_L$ partitions Σ^* into a collection of equivalence classes.

Definition

L: *A language For a string* $x \in \Sigma^*$, *let*

$$[x] = [x]_L = \{ y \in \Sigma^* \mid x \equiv_L y \}$$

be the equivalence class *of* x *according to* L.

Definition

$[L] = \{ [x]_L \mid x \in \Sigma^* \}$ *is the set of* equivalence classes *of* L.

Strings in the same equivalence class are indistinguishable

Lemma

Let x, y be two distinct strings.
$x \equiv_L y \iff x, y$ are indistinguishable for L.

Proof.

$x \equiv_L y \implies \forall w \in \Sigma^*: xw \in L \iff yw \in L$
x and y are indistinguishable for L.

$x \not\equiv_L y \implies \exists w \in \Sigma^*: xw \in L$ and $yw \notin L$
$\implies x$ and y are distinguishable for L.

□

Strings in the same equivalence class are indistinguishable

Lemma

Let x, y be two distinct strings.
$x \equiv_L y \iff x, y$ are indistinguishable for L.

Proof.

$x \equiv_L y \implies \forall w \in \Sigma^*: xw \in L \iff yw \in L$
x and y are indistinguishable for L.

$x \not\equiv_L y \implies \exists w \in \Sigma^*: xw \in L$ and $yw \notin L$
$\implies x$ and y are distinguishable for L.

□

Strings in the same equivalence class are indistinguishable

Lemma

Let x, y *be two distinct strings.*

$x \equiv_L y \iff x, y$ *are indistinguishable for* L*.*

Proof.

$x \equiv_L y \implies \forall w \in \Sigma^*: xw \in L \iff yw \in L$

x and y are indistinguishable for L.

$x \not\equiv_L y \implies \exists w \in \Sigma^*: xw \in L$ and $yw \notin L$

$\implies x$ and y are distinguishable for L.

Strings in the same equivalence class are indistinguishable

Lemma

Let x, y be two distinct strings.
$x \equiv_L y \iff x, y$ *are indistinguishable for* L.

Proof.

$x \equiv_L y \implies \forall w \in \Sigma^*: xw \in L \iff yw \in L$
x and y are indistinguishable for L.

$x \not\equiv_L y \implies \exists w \in \Sigma^*: xw \in L$ and $yw \notin L$
$\implies x$ and y are distinguishable for L.

Strings in the same equivalence class are indistinguishable

Lemma

Let x, y be two distinct strings.
$x \equiv_L y \iff x, y$ *are indistinguishable for* L.

Proof.

$x \equiv_L y \implies \forall w \in \Sigma^*\colon xw \in L \iff yw \in L$
x and y are indistinguishable for L.

$x \not\equiv_L y \implies \exists w \in \Sigma^*\colon xw \in L$ and $yw \notin L$
$\implies x$ and y are distinguishable for L.

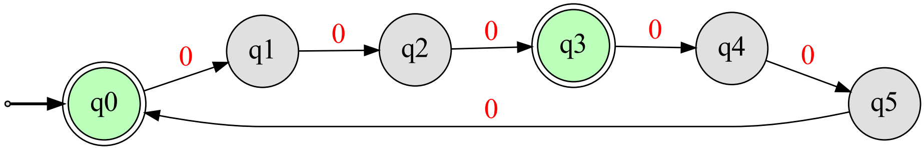
□

All strings arriving at a state are in the same class

Lemma

$M = (Q, \Sigma, \delta, s, A)$ a DFA for a language L.
For any $q \in A$, let $L_q = \{w \in \Sigma^* \mid \nabla w = \delta^*(s, w) = q\}$.
Then, there exists a string x, such that $L_q \subseteq [x]_L$.

An inefficient automata



THE END

...

(for now)