Myhill Nerode Theorem

Equivalence Relation

- Def: Assume R is a relation on a set A, that is, $R \subseteq A \times A$. We write aRb which means $(a,b) \in R$ to indicate that a is related to b via the relation R:
  - R is reflexive if for every $a \in A$, aRa
  - R is symmetric if for every a and b in A, if aRb, then bRa
  - R is transitive if for every a, b, and c in A, if aRb and bRc, then aRc
  - R is an equivalence relation on A if R is reflexive, symmetric, and transitive

Equivalence Class

- Suppose R is any equivalence relation on A. For any element a of A, we denote by $[a]_R$, or sometimes simply by $[a]$, the equivalence class containing a, that is,

$$[a]_R = \{x \in A \mid xRa\}$$

- Thm: For any partition C of a set A, the relation R on A, defined by xRy $\Leftrightarrow$ x and y belong to the same element of C, is an equivalence relation on A.

  Conversely, if R is any equivalence relation on A, the set of equivalence classes is a partition of A, and two elements of A are equivalent $\Leftrightarrow$ they are in the same equivalence class.

Distinguishing One String from Another

- Def:

  Let L be a language over Σ

  Two strings x and y in Σ^* are distinguishable with respect to L if there is a string $z \in \Sigma^*$ (which may depend on x and y) so that exactly one of the strings xz and yz is in L

  The string z is said to distinguish x and y with respect to L

- We may say that x and y are indistinguishable with respect to L if there is no such string z;
- In other words, if for every z, both xz and yz have the same status---either both in L or both not in L

Eg: $L=\{x \in \{0,1\}^* \mid x \text{ ends with } 10\}$

the strings 01011 and 100 are distinguishable with respect to L because for z=0, $01011z \in L$ and $100z \notin L$.

The strings 0 and 100 are indistinguishable with respect to L

- Lemma

  Suppose that $L \subseteq \Sigma^*$ and $M=(Q, \Sigma, q_0, F, \delta)$ is any FA recognizing L.

  If x and y are two strings in Σ^* for which $\delta^*(q_0,x)=\delta^*(q_0,y)$, then x and y are indistinguishable with respect to L

Proof:

Let z be any string in Σ^* , and consider the two strings xz and yz.

$$\delta^*(q_0,xz)= \delta^*(\delta^*(q_0,x),z)$$

$$\delta^*(q_0,yz)= \delta^*(\delta^*(q_0,y),z)$$

and therefore, by our assumption, $\delta^*(q_0,xz)=\delta^*(q_0,yz)$. Since M is assumed to recognize L, these two strings are either both in L or both not in L. Therefore, x and y are indistinguishable with respect to L.

■

- Thm 1

  Suppose that $L \subseteq \Sigma^*$ and, for some positive integer n, there are n strings in Σ^* , any two of which are distinguishable with respect to L. Then there can be no FA recognizing L with fewer than n states.

Proof:

- Suppose that $x_1, x_2, \ldots, x_n$ are n strings, any two of which are distinguishable with respect to L.
- If $M=(Q, \Sigma, q_0, A, \delta)$ is any FA with fewer than n states, then by the pigeonhole principle, the states $\delta^*(q_0,x_1)$, $\delta^*(q_0,x_2)$, …, $\delta^*(q_0,x_n)$ cannot all be distinct, and so for some $i \neq j$, $\delta^*(q_0,x_i) = \delta^*(q_0,x_j)$.

  Since x_i and x_j are distinguishable with respect to L, M cannot recognize L. ∎

A Criterion for Regularity

- Def

  Let L be any language in Σ^* . The relation I_L on Σ^* (the indistinguishability relation) is defined as follows:
  For any two strings $x,y \in \Sigma^*$, $x \; I_L \; y \Leftrightarrow$ x and y are indistinguishable with respect to L.

  In other words, $x \; I_L \; y$ if , for any $z \in \Sigma^*$, either xz and yz are both in L, or xz and yz are both in L'

- Lemma

  For any language L, I_L is an equivalence relation on Σ^*

Proof:

It is obvious that I_L is reflexive and symmetric.
Suppose x I_L y and y I_L w. We must show that x I_L w.
Let z be any string in Σ^* . If xz $\in$L, then yz $\in$L, since x I_L y, and therefore wz $\in$L, since y I_L w.

Similarly, if xz$\notin$ L, then wz$\notin$ L.

Therefore x I_L w.

- Assume L is a regular language, and FA $M=(Q, \Sigma , q_0, F, \delta)$ recognizes L. If $q\in Q$, we let

$$L_q=\{x\in \Sigma^* | \delta^*(q_0,x)=q \}$$

- If we start with an equivalence class q containing a string x, then $\delta(q,a)$ should be the equivalence class containing xa, that is

$$\delta([x],a)=[xa]$$

- Lemma:

  I_L is right invariant with respect to concatenation. In other words, for any $x,y\in\Sigma^*$ and any $a\in\Sigma$, if $x\ I_L\ y$, then $xa\ I_L\ ya$. Equivalently, if $[x]=[y]$, then $[xa]=[ya]$

Proof:

Suppose that $x\ I_L\ y$ and $a\in\Sigma$. For any $z' \in\Sigma^*$, xz' and yz' are either both in L or both not in L. With $z'=az$, we complete our proof.

■

- Thm 2

  Let $L \subseteq \Sigma^*$, and let Q_L be the set of equivalence classes of the relation I_L on Σ^* .

  If Q_L is a finite set, then $M_L=(Q_L, \Sigma, q_0, F_L, \delta)$ is a finite automaton accepting L, where $q_0=[\in]$, $F_L=\{q\in Q_L \mid q\cap L\neq\emptyset\}$ and $\delta : Q_L \times \Sigma \rightarrow Q_L$ is defined by the formula $\delta([x],a)=[xa]$.

  Furthermore, M_L has the fewest states of any FA accepting L.

Proof:

(1) By the previous lemma, $\delta([x],a)=[xa]$ is a meaningful definition.

To verify that M_L recognizes L, need to prove $\delta^*([x], y)=[xy]$, for any x, y.

By induction, it is clear for $y=\Lambda$. Suppose it is true for some y.

Consider $\delta^*([x], ya)= \delta(\delta^*([x], y), a)= \delta([xy], a) = [xya]$.

Thus $\delta^*(q_0, x)= \delta^*([\Lambda], x) =[x]$.

Since $F_L=\{q\in Q_L \mid q\cap L\neq\varnothing\}$, M_L accepts x iff $[x]\cap L\neq\varnothing$.

It is clear that if $x\in L$, then $[x]\cap L\neq\varnothing$.

On the other hand, if [x] contains y of L, then x must be in L; otherwise Λ will distinguish x and y. Therefore, M_L accepts L.

(2) If there are n equivalence classes of I_L, then there are n pair-wise distinguishable strings. By a previous theorem, any FA accepting L has at least n states. M_L has exactly n states, it has the fewest possible.

- Corollary: (Myhill-Nerode theorem)
  L is a regular language ⇔
  The set of equivalence classes of I_L is finite

Proof:

Follow from the Theorem 1 and Theorem 2

■

Example

- Let EVEN-ODD be the set of strings over {a,b} with an even number of a's and an odd number of b's
  - Is the string aa distinguishable from the string bb with respect to EVEN-ODD?
  - Is the string aa distinguishable from the string ab with respect to EVEN-ODD?

Definition of equivalence classes

- Every language L *partitions* Σ^* into equivalence classes via indistinguishability
  - Two strings x and y belong to the same equivalence class defined by L iff x and y are indistinguishable w.r.t L
  - Two strings x and y belong to different equivalence classes defined by L iff x and y are distinguishable w.r.t. L

Example

How does EVEN-ODD partition {a,b}* into equivalence classes?

Strings with an EVEN number of a's and an EVEN number of b's	Strings with an ODD number of a's and an EVEN number of b's
Strings with an EVEN number of a's and an ODD number of b's	Strings with an ODD number of a's and an ODD number of b's

Second Example

Let 1MOD3 be the set of strings over {a,b} whose length mod 3
How does 1MOD3 partition {a,b}* into equivalence classes?

Length mod 3 = 0

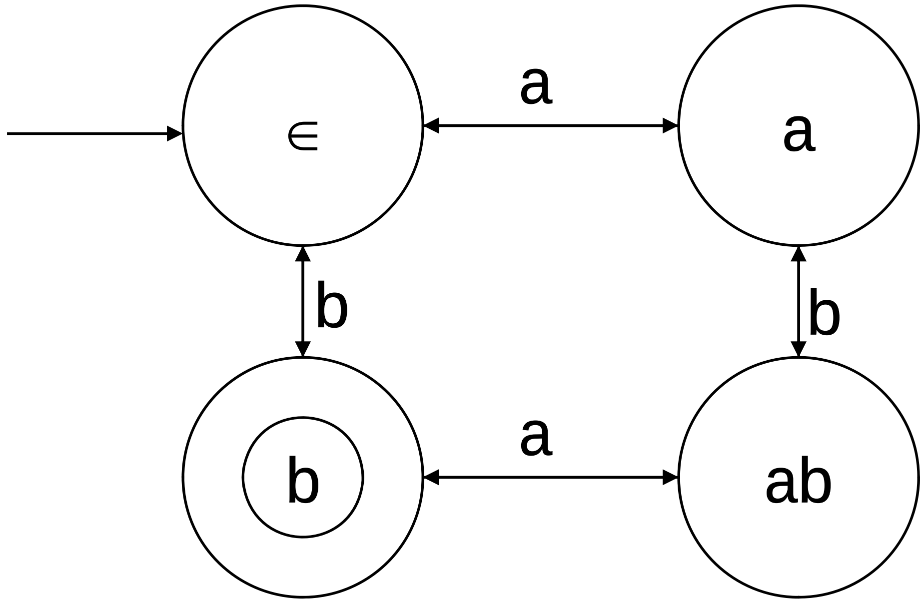
Length mod 3 = 1

Length mod 3 = 2

Designing FSA’s

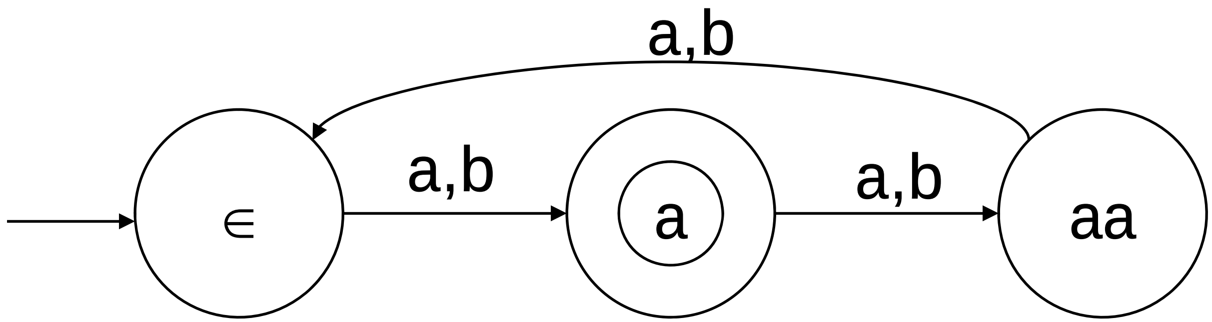
Designing an FSA for EVEN-ODD

Even Even	Odd Even
Even Odd	Odd Odd



Designing an FSA for 1MOD3

Length mod 3 = 0
Length mod 3 = 1
Length mod 3 = 2



Proving a language is not regular

Third Example

- Let EQUAL be the set of strings x over {a,b} s.t. the number of a's in x = the number of b's in x
- How does EQUAL partition {a,b}* into equivalence classes?
  - Strings with an equal number of a's and b's
  - Strings with one extra a
  - Strings with one extra b
  - Strings with two extra a's
  - Strings with two extra b's
  - ...
- There are an *infinite* number of equivalence classes.
  - Can we construct a *finite* state automaton for EQUAL?
  - We shall see that the answer is no.

- Eg: Let $L=\{0^n1^n|n\geq 0\}$.
  - The intuitive reason L is not regular :
    we must remember how many 0's we have seen
  - $S=\{0^n|n\geq 0\}$: infinite set 0^i , $0^j \in S$, $i\neq j$
    $0^i1^i\in L$ but $0^j1^i\notin L$.
    $\Rightarrow$ 1^i distinguishes 0^i and 0^j
    $\Rightarrow$ The relation I_L has infinitely many distinct equivalence classes and that L is not regular.

- Eg:

  $S=\{0^n|n\geq 0\}$:infinite set, and $L=\{ww|w\in\{0,1\}^*\}$ is a language.

  $z=1^n0^n1^n$ is a string.

  $\Rightarrow$ $0^nz \in L$, $0^mz \notin L$

  $\Rightarrow$ z distinguishes 0^n and 0^m