Mathematical Foundation of Computer Sciences II

Algorithms on Finite Automata

Guoqiang Li

School of Software, Shanghai Jiao Tong University

Automata as Models

Models and Specifications

A finite automaton can be used to describe behaviours of a system or an (intra-procedure) program. Thus regarded it as a model $\mathcal{M}$.

A finite automaton can also be used to describe regulations of a system or an (intra-procedure) program. Thus regarded it as a specification φ.

Usually, we should guarantee

$$\mathcal{M} \models \varphi$$

In the automata terminology, we should guarantee

$$L(\mathcal{M}) \subseteq L(\varphi)$$

An Algorithmic Problem of FA

Given two automata M and N,

$$L(M) \subseteq L(N)$$

Two approaches:

$$L(M) \cap L(N^c) = \emptyset$$

and,

$$L(M^c) \cup L(N) = \Sigma^*$$

New Algorithmic Operations

New Operations

intersection

complement

emptiness

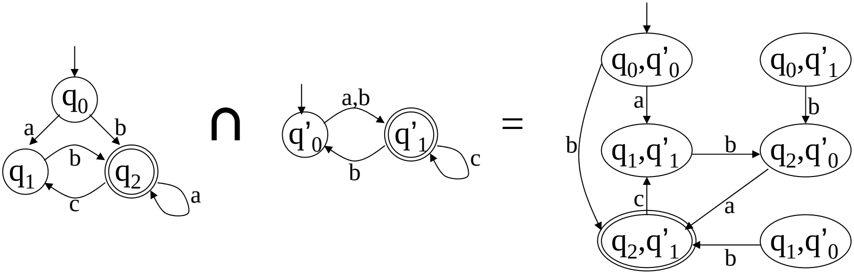
universality

Intersection of Automata

$A = (S, \Sigma, \delta, q_0, F), B = (S', \Sigma, \delta', q'_0, F')$

An Automaton that accepts $L(A) \cap L(B)$

$$(S \times S', \Sigma, \delta \times \delta', (q_0, q'_0), F \times F')$$



Complement of Automata

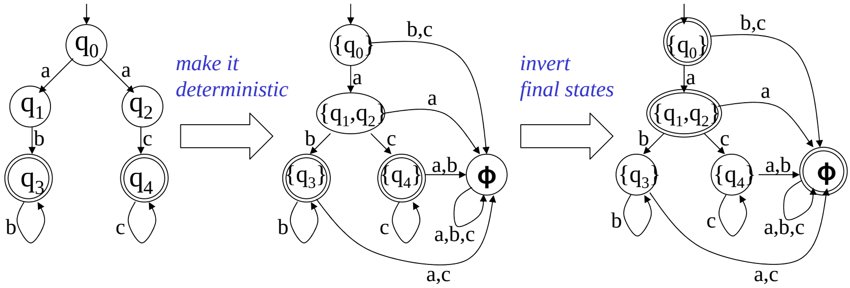
$A = (S, \Sigma, \delta, q_0, F)$

- if A is deterministic, $A^c = (S, \Sigma, \delta, q_0, S - F)$.
- if A is non-deterministic, make A deterministic first

  Assume that A is without ε-transition. Then

  $$(P(S), \Sigma, \{(X, a, \{y \mid x \xrightarrow{a} y \text{ for } x \in X\})\}, \{q_0\}, \{X \mid X \cap F = \emptyset\})$$

Example of Complement



Pumping Lemma

Pumping Lemma

Let $A = (Q, \Sigma, \delta, q_0, F)$ be a finite automaton. For each $z \in L(A)$ with $|z| \geq |Q|$, $\exists u, v, w$ such that

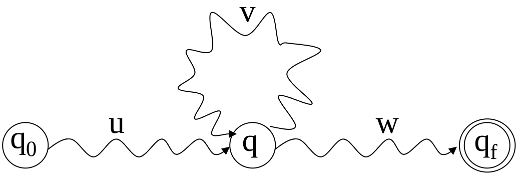
1. $z = uvw$,
2. $|uv| \leq |Q|$,
3. $|v| \geq 1$, and
4. $uv^i w \in L(A)$.

Idea of Pumping Lemma

Pumping Lemma

Let $A = (Q, \Sigma, \delta, q_0, F)$ be a finite automaton. For each $z \in L(A)$ with $|z| \geq |Q|$, $\exists u, v, w$ such that

1. $z = uvw$,
2. $|uv| \leq |Q|$,
3. $|v| \geq 1$, and
4. $uv^i w \in L(A)$.



Pigeon hole principle!

Proof

Let $A = (Q, \Sigma, \delta, q_0, F)$ be a DFA recognizing L. Let $s = s_1 s_2 \ldots s_n$ be a string in L with $n \geq |Q|$. Let $r_1, \ldots, r_{n+1}$ be the sequence of states that A enters while processing s, i.e.,

$$r_{i+1} = \delta(r_i, s_i)$$

for $i \in [n]$.

Among the first $|Q| + 1$ states in the sequence, two must be the same, say r_j and r_l with $j < l \leq |Q| + 1$. We define

$$u = s_1 \ldots s_{j-1}, v = s_j \ldots s_{l-1}, \text{ and } w = s_l \ldots s_n$$

Generalization of Pumping Lemma

Pumping Lemma

Let $A = (Q, \Sigma, \delta, q_0, F)$ be a finite automaton. There exist a number p, named the pumping length, For each $z \in L(A)$ with $|z| \geq p$, $\exists u, v, w$ such that

1. $z = uvw$,
2. $|uv| \leq p$,
3. $|v| \geq 1$, and
4. $uv^iw \in L(A)$.

Example

The language $L =| \{0^n 1^n \mid n \geq 0\}$ is not regular.

Proof.

If it is regular, consider $s = 0^p 1^p$. By the Pumping lemma, $s = uvw$ with $uv^i w \in L$ for all $i \geq 0$.

As $|uv| \leq p$ and $|v| > 0$, $v = 0^i$ for some $i > 0$. But then $uw = 0^{n-i} 1^n \notin L$. Contradicting the lemma.

Quiz

The language $L = \{w \mid w \text{ has an equal number of 0s and 1s }\}$ is not regular.

The language $L = \{ww \mid w \in \{0,1\}^*\}$ is not regular.

The language $L = \{0^m 1^n \mid m \neq n\}$ is not regular.

Emptiness

Theorem

$L(A) \neq \emptyset$ *iff* $\exists z$ *with* $|z| < |Q|$ *and* $z \in L$.

Complexity of Subset

$A = (S, \Sigma, \delta, q_0, F)$, $B = (S', \Sigma, \delta', q_0', F')$

Ask $L(A) \subseteq L(B)$?

$$L(A) \subseteq L(B) \Leftrightarrow L(A) \cap L(B^c) = \emptyset$$

What is the complexity of the subset?

Myhill-Nerode Theorem

Equivalence Relation

A binary relation R on a set S is a subset of $S \times S$. An equivalence relation on a set satisfies

- Reflexivity: For all x in S, xRx
- Symmetry: For $x, y \in S$, $xRy \Leftrightarrow yRx$
- Transitivity: For $x, y, z \in S$, $xRy \wedge yRz \Rightarrow xRz$

Every equivalence relation on S partitions S into equivalence classes. The number of equivalence classes is called the index of the relation.

Quiz

Let $S = \Sigma^+$ where $\Sigma = \{a, b\}$.

Define R as xRy whenever x and y both end in the same symbol of Σ.

How many equivalence classes does R partition S into?

Right Invariance

An equivalence relation on Σ^* is said to be right invariant with respect to concatenation if $\forall x, y \in \Sigma^*$ and $a \in \Sigma$, xRy implies that $xaRya$.

Quiz

Let $S = \Sigma^*$ where $\Sigma = \{a, b\}$ and R be defined as follows:

xRy if x and y have the same number of a's.

- How many equivalence classes does R partition S into?
- Is R right invariant?

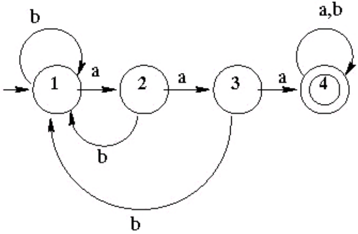
Equivalence Relations Induced by DFA's

Let $M = (Q, \Sigma, \delta, q_0, F)$ be a DFA.

Define a relation R_M as follows: For $x, y \in \Sigma^*, xR_My \Leftrightarrow \delta^*(q_0, x) = \delta^*(q_0, y)$

- Is this an equivalence relation?
- If so, how many equivalence classes does it have? iow., what is its index?

An Example



C1: All strings not containing more than 2 consecutive *a*'s and which end in *a* or *b*.

C2: All strings not containing more than 2 consecutive *a*'s and which end in *a*.

C3: All strings not containing more than 2 consecutive *a*'s and which end in *aa*.

C4: All strings containing at least three consecutive *a*'s.

Congruence

$u \, R \, v$ is a congruence iff R is an equivalence and preserved under concatenation

$$u \, R \, v \Rightarrow wuw' \, R \, wvw' \text{ for each } w, w' \in \Sigma^*$$

.

Myhill-Nerode Theorem

Myhill-Nerode Theorem

The following three statements are equivalent.

1. L is regular.
2. L is a union of congruence classes of finite index.
3. R_L is a congruence of finite index, where

$$u \, R_L \, v \text{ iff } uw \in L \Leftrightarrow vw \in L \text{ for each } w \in \Sigma^*$$

Proof: $3 \Rightarrow 1$

Let R_L be a congruence of finite index, where

$$u\,R_L\,v \text{ iff } uw \in L \Leftrightarrow vw \in L \text{ for each } w \in \Sigma^*$$

Let an automaton $A = (Q, \Sigma, \delta, q_0, F)$ be

- $Q = \Sigma^*/R_L$ (finite congruence classes of R_L)
- $\delta = \{([u], a, [ua]) \mid u \in \Sigma^*, a \in \Sigma\}$
- $q_0 = [\varepsilon]$
- $F = \{[u] \mid u \in L\}$

$L = L(A)$ and L is regular.

Proof: $1 \Rightarrow 2$

Let $L = L(A)$ with $A = (Q, \Sigma, \delta, q_0, F)$

$u \, R_A \, v$ iff $q \xrightarrow{u} q' \Leftrightarrow q \xrightarrow{v} q'$ for $q, q' \in Q$

R_A is a congruence of finite index, (at most $2^{|Q| \times |Q|}$).

Proof: $2 \Rightarrow 3$

Let R be a congruence of finite index and let L be a union of congruence classes.

Let $u \, R_L \, v$ iff $uw \in L \Leftrightarrow vw \in L$ for each $w \in \Sigma^*$.

$u \, R \, v \Rightarrow u \, R_L \, v$; thus, R_L is of finite index.

Another Technique for Complement

Myhill-Nerode Theorem says that L is regular $\Leftrightarrow$ L is a union of congruence classes of finite index.

$$L = \bigcup_{U_i \cap L \neq \emptyset} U_i$$

Note that each U_i is regular! Thus,

$$L^c = \bigcup_{U_i \cap L = \emptyset} U_i$$

Other Computations

Other Computations

minimization

equivalence

bisimulation

reversal

homomorphism

inverse homomorphism

...

Assignment 1

Assignment 1

Exercises 1.5 (b, d); 1.6 (e, i); 1.11; 1.14 (b); 1.29; 1.38; 1.47; 1.48

deadline Mar. 18