

Topics

1. Deterministic Finite State Automata (DFA, FSA, FA)
2. Nondeterministic Finite State Automata (NFA, NFA)
3. Regular Languages and Regular Expressions
4. Regular Grammars
5. Minimal Deterministic Finite State Machines

Slide Lecture 1 –2

More Topics

6. Pushdown Stack Machines and Context Free Grammars
7. Parsing
8. Turing Machines
9. Undecidibility: The Halting Problem
10. P and NP Problems and NP Completeness

Slide Lecture 1 –4

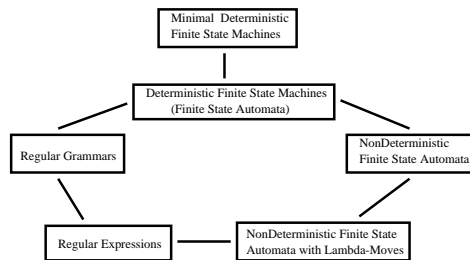


Figure 1: Finite State Machines

Slide Lecture 1 –3

Basics: Sets

A set is ...

$A = \{1, 3, 5, 7, 11, \dots\}$

$B = \{x \mid x \text{ is a prime number}\}$

$y \in B$

$A \subset B$

$A \subseteq B$

Slide Lecture 1 –5

Basics: Set Operators

Complement	A'
Union	$A \cup B$
Intersection	$A \cap B$
Difference	$A - B$
Symmetric Difference	$A \oplus B$
Cartesian Product	$A \times B$
Power set	2^A

Slide Lecture 1 -6

The **THEORY OF COMPUTABILITY** is the mathematical study of computing machines and their capabilities.

Data are modeled as strings of symbols.

An *alphabet* is defined as a finite set of symbols:

Roman alphabet $\{a, b, \dots, z\}$

Decimal alphabet $\{0, 1, \dots, 9\}$

A **string** is a finite sequence of symbols.

Words in the English language are strings by this definition.

Unsigned integers are strings over the decimal alphabet.

Slide Lecture 1 -8

Basics: Set Laws

Commutative: $A \cup B = B \cup A, A \cap B = B \cap A$

Associative: $A \cup (B \cup C) = (A \cup B) \cup C$

Distributive: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

DeMorgan's: $(A \cup B)' = A' \cap B', (A \cap B)' = A' \cup B'$

Empty set: $A \cup \emptyset = A, A \cap \emptyset = \emptyset$

Slide Lecture 1 -7

The **length** of a string x is denoted $|x|$.

A zero-length string is called the **empty** or **null** string, and is often denoted Λ or ϵ .

Note: this is not the same as the empty set, denoted \emptyset .

The set of all strings of length 1 or more over alphabet Σ is denoted Σ^+

Slide Lecture 1 -9

If $\Sigma = \{0, 1\}$

Σ^+ is the positive closure, the set of all binary strings

$\Sigma^+ = \{0, 1, 00, 01, 10, 11, \dots\}$

When Σ^+ is extended to include the empty string it is denoted Σ^*

$$\Sigma^* = \Sigma^+ \cup \{\Lambda\}$$

What is the difference between the empty string and the empty set?

What is the positive closure?

Slide Lecture 1 -10

Λ is a substring of every string, including Λ

If $w = xv$, v is a **suffix** of w

If $w = vy$, v is a **prefix** of w

Suffixes and prefixes are **proper** when the root is not Λ

We can inductively create strings from a given string w

$$w^i = w_1 w_2 \dots w_i$$

where i is a non-negative integer.

Let $w = \text{"da"}$ $w^2 = \text{"dada"}$

Slide Lecture 1 -12

The symbol at position i in a string is referred to as the i^{th} symbol and is denoted $x(i)$

If $x = 10111$

$$x(1) = 1 \quad x(2) = 0 \quad x(3) = 1 \quad \text{etc.}$$

OPERATIONS ON STRINGS

Let x and y be strings

Concatenation is denoted $x \cdot y$ or simply xy

If $x = \text{"every"}$ and $y = \text{"one"}$

$$xy = \text{everyone} \quad yx = \text{oneevery}$$

Concatenation is associative.

$$(wx)y = w(xy)$$

Slide Lecture 1 -11

w^R is defined as:

1. If $w = \lambda$, $w^R = \lambda$

2. If $w = x$, $w^R = x$

3. If $w = vx$ where $v \in \Sigma$, $x \in \Sigma^*$ then $w^R = (x^R)v$

w^R is just w backwards.

The set of **palindromes** is defined as

$$\{w | w = w^R\}$$

Examples:

"bob" "1881" "able was I ere I saw Elba"

Slide Lecture 1 -13

A **Language** is a set of strings over an alphabet Σ ; it is $\subseteq \Sigma^*$.

Languages can be represented using set notation since they are discrete sets.

$$L = \{w \in \Sigma^* \mid w \text{ has property } p\}$$

Let $\Sigma = \{0, 1, \dots, 9\}$

The palindromic integers

$$\{w \in \Sigma^* \mid w = w^R\}$$

Slide Lecture 1 -14

For any alphabet Σ , a language $L \subseteq \Sigma^*$ is a countable set since Σ^* is countable using a **lexicographic ordering**.

We enumerate the strings of Σ^* in lexicographic order:

1. all strings of length k ($k \geq 0$) precede strings of length m if $m > k$ (λ is the least element)
2. the n^k strings of length k are ordered according to a symbol-wise relation imposed on Σ ,
 $\Sigma = \{\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n\}$

Slide Lecture 1 -16

Language Operations

L^k is the set of all strings obtained by concatenating k elements of L .

Kleene *:

$$L^* = \bigcup_{k=0}^{\infty} L^k$$

and

$$L^+ = \bigcup_{k=1}^{\infty} L^k$$

Slide Lecture 1 -15

Given two strings of equal length, $x \leq y$ iff

$$x = qw \text{ and}$$

$$y = qv \text{ and}$$

$$w \leq v$$

for some $q, w, v \in \Sigma^*$

Slide Lecture 1 -17

Let $\Sigma_1 = \{a, b, \dots, z\}$

$ace < able$... not alphabetic

Let $\Sigma_2 = \{0, 1\}$

$0001 > 101$... not by magnitude

What about $L = \{xy \mid x \in (\Sigma_2 - \{0\}), y \in \Sigma_2^*\}$
for $\Sigma_2 = \{0, 1\}$

binary strings with no leading zeros!

Slide Lecture 1 -18

The central property of equivalence relations is that they partition some set A into a collection of disjoint sets.

Why do we care?

We will use this to

1. show equivalence of machines
2. show equivalence of states in machines
3. reduce machines (a machine is **minimal** if it does not contain equivalent states)

Common non-mathematical equivalence relations:

$R_1 =$ "lives in the same house as"

$R_2 =$ "computes the same function as"

Slide Lecture 1 -20

Properties of Relations

(S is a set, R is a relation)

reflexive:

$$aRa \text{ for all } a \in S$$

transitive:

$$aRb \wedge bRc \Rightarrow aRc$$

symmetric:

$$aRb \Rightarrow bRa$$

A relation that is reflexive, transitive, and symmetric is an

equivalence relation

Slide Lecture 1 -19

Proof Techniques

Constructive Proof "There exists z such that..."

Proof by Contrapositive $(p \rightarrow q) = (\neg q \rightarrow \neg p)$

Proof by Contradiction Assume $\neg p$ and show that something known to be true must then be false

Proof by Cases subdivide into exhaustive set of possibilities and prove each separately

Slide Lecture 1 -21

Inductive Proofs

1. Basic step:
show $1 \in X$, i.e, show $P(1)$ is true
2. Inductive hypothesis:
assume that for some n
 $P(1) \wedge P(2) \wedge \dots \wedge P(n)$ is true
3. The inductive step:
show $P(n+1)$ is true

Then, by the inductive principle,
 $P(n)$ is true for all $n \in \mathbb{N}$

Slide Lecture 1 -22

Example I (cont.)

Theorem: the sum of the first n odd natural numbers is
 n^2

Prove: $\sum_{i=1}^{m+1} 2i - 1 = (m+1)^2$

Note: $\sum_{i=1}^{m+1} 2i - 1 = \sum_{i=1}^m 2i - 1 + (2(m+1) - 1)$
 $= m^2 + 2m + 1$
 $= (m+1)^2$

We will use induction for language descriptions.

Slide Lecture 1 -24

Example I

Theorem:

the sum of the first n odd natural numbers is n^2

$$\sum_{i=1}^n 2i - 1 = n^2$$

1. Basis: $\sum_{i=1}^1 2i - 1 = 2 - 1 = 1 = 1^2$
2. Hypothesis: For all $n \leq m$ Assume
 $\sum_{i=1}^n 2i - 1 = n^2$
3. Inductive step: consider $n = (m+1)$

Slide Lecture 1 -23

Diagonalization

Let R be a binary relation on a set X , and define D (the diagonal set for R) as

$$\{x \mid x \in X \text{ and } (x, x) \notin R\}$$

For each $x \in X$,

$$\text{let } Rx = \{y \mid y \in X \text{ and } (x, y) \in R\}$$

Then for any $x \in X$,

$$Rx \text{ is distinct from } D$$

This applies to finite or infinite sets.

Slide Lecture 1 -25

Let X be a finite set.

We can represent the relation R as an $n \times n$ Boolean matrix, where $n = |X|$, such that the (i, j) entry is true iff $(x_i, x_j) \in R$.

The set D then can be viewed as the “complement” of the n -element diagonal.

Let Rx_i represent the i^{th} column (or row) of the matrix. Notice that the diagonal is distinct from any column: this is the essence of the

diagonalization principle.

Slide Lecture 1 –26

COUNTABLY INFINITE

refers to a set that can be mapped “onto” the natural numbers in a “one-to-one” fashion, i.e., there is a bijection

$$f : N \rightarrow X$$

UNCOUNTABLY INFINITE:

no bijection exists such that $f : N \rightarrow X$

CLAIM:

The power set of the natural numbers is uncountable.

PROOF BY DIAGONALIZATION AND CONTRADICTION

Slide Lecture 1 –28

Example: Let $X = \{a b c d\}$

and $R = \{(a, b), (a, d), (b, b), (b, c), (c, c), (d, b), (d, c)\}$

	a	b	c	d
a	0	1	0	1
b	0	1	1	0
c	0	0	1	0
d	0	1	1	0

The diagonal vector is 0 1 1 0

and its complement $D = 1 0 0 1$

D differs from every column or row in at least one position.

Slide Lecture 1 –27

Assume the power set of the natural numbers is countably infinite.

THIS IMPLIES A BIJECTION $f : N \rightarrow 2^N$

$2^N = \{S_1, S_2, \dots\}$ where $f(i) = S_i$

Now consider $D = \{n \in N | n \notin S_n\}$

D is clearly a subset of the natural numbers.

Since $S_i \in 2^N$, it represents all natural numbers and there exists natural number k such that $D = S_k$.

Assuming the power set countable implies that

$$D = S_k$$

Slide Lecture 1 –29

But by the diagonalization principle this is not true.
 If the power set of the natural numbers is countably infinite, we must be able to map it to the natural numbers.

Assume $k \in S_k$.

Since $D = \{n | n \notin S_n\}$

$$k \notin D$$

But $D = S_k \dots$ contradiction: POWER SET IS UNCOUNTABLY INFINITE

The problem is that the definition of the diagonal contradicts the requirement of countability. So therefore by contradiction, the power set is not countably infinite.

Slide Lecture 1 -30

The set of ordered pairs of natural numbers is denumerable (countably infinite)

	0	1	2	3	...
0	[0, 0]	[0, 1]	[0, 2]	[0, 3]	...
1	[1, 0]	[1, 1]	[1, 2]	[1, 3]	...
2	[2, 0]	[2, 1]	[2, 2]	[2, 3]	...
3	[3, 0]	[3, 1]	[3, 2]	[3, 3]	...
4	[4, 0]	[4, 1]	...		

Slide Lecture 1 -32

	S_0	S_1	S_2	$S_3 \dots$
1	0	1	0	1
2	1	0	1	0
3	0	0	0	1
4	1	1	0	1

$D = 1110 =$ complement of diagonal

$j \in D$ iff $j \notin N_j$

Since $S_0 S_1 S_2 \dots S_\infty$ is exhaustive, $D = S_i$ for some i but since $j \in D$ iff $j \notin N_j$, $j \in N_j$ iff $j \notin N_j \dots$ contradiction.

Slide Lecture 1 -31

The set of possible functions is uncountably infinite

	f_0	f_1	f_2	f_3	...
0	$f_0(0)$	$f_1(0)$	$f_2(0)$	$f_3(0)$...
1	$f_0(1)$	$f_1(1)$	$f_2(1)$	$f_3(1)$...
2	$f_0(2)$	$f_1(2)$	$f_2(2)$	$f_3(2)$...
3	$f_0(3)$	$f_1(3)$	$f_2(3)$	$f_3(3)$...
4	$f_0(4)$	$f_1(4)$...		

Assume f_0 to f_∞ contains all functions. Let function G be such that $G(i) = f_i(i) + 1$. Then G differs from every function f_i . Thus f_0 to f_∞ is not all possible functions.

Therefore the set f of possible functions is uncountable.

Slide Lecture 1 -33

The set of rational numbers (which can be expressed as p/q , where p and q are natural numbers, $q \neq 0$) is countably infinite.

	1	2	3	4	...
1	1/1	2/1	3/1	4/1	...
2	1/2	2/2	3/2	4/2	...
3	1/3	2/3	3/3	4/3	...
4	1/4	2/4	3/4	4/4	...
5	1/5	2/5	...		

Slide Lecture 1 -34

Recursive Definitions on Languages

Example:

Let Σ be the alphabet $(,), *, a, b$.

The language L is defined by:

1. $a \in L, b \in L, () \in L$
2. For any $x, y \in L, (*xy) \in L$
3. No string is in L unless it can be obtained using rules 1 and 2.

Slide Lecture 1 -36

Recursive Definitions

Example:

Base case: $A(1, m) = m$

Recursive case: $A(n, m) = m + A(n - 1, m)$

Slide Lecture 1 -35