CS 331a

Foundations of Computer Science

Course Notes

Instructor *Sheng Yu*

Department of Computer Science
University of Western Ontario
London, Ontario

Course Structure:

1 <u>Background knowledge</u>

sets, multisets, sequences, functions, relations, proof methods, proof techniques, alphabets, words, languages

2 <u>Finite automata</u>

nondeterministic finite automata (NFA), deterministic finite automata (DFA), transformation from NFA to DFA, properties of FA languages, pumping lemma

3 <u>Regular expressions</u>

equivalence of regular expressions and finite automata (in defining languages)

4 **Context-free grammars**

simplification and normal forms, general parsing algorithms, pumping lemma and other properties

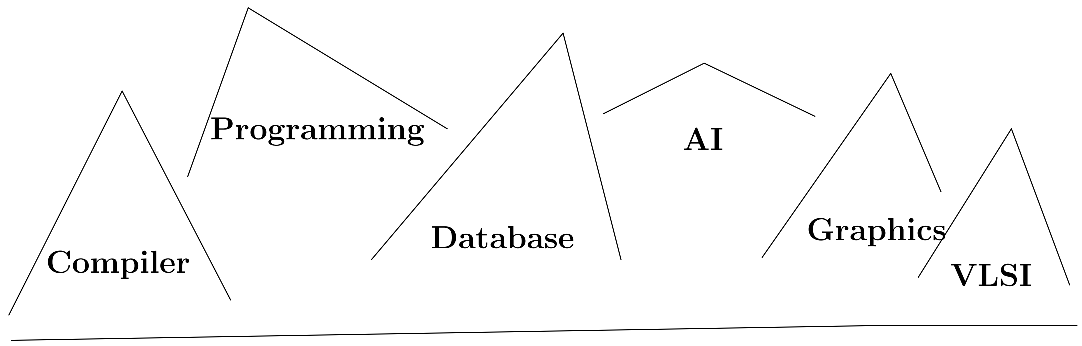
5 **Pushdown automata**

nondeterministic pushdown automata (NPDA), deterministic pushdown automata (DPDA), PDA vs. CFGs

6 **Turing machines**

various types of TMs, universal TMs, decidability and undecidability, time and space complexities

Motivation Of the Study



Theory of Computing

(1) Computability

(2) Complexity

(3) Software design

(4) Circuit design

....

I. Background Knowledge

1. Sets

1) A set is a collection of elements taken from some universe.

2) A set is finite if it contains a finite number of elements and is infinite otherwise.

3) The cardinality of a set is the number of elements in the set, denoted by $\#A$ or $|A|$ (for the set A).

– **How to specify a set:**

(1) **List all the members:**

$\{\}$ (or $\emptyset$),

$A = \{2,\ 3,\ 5,\ 7\}$,

$B = \{3,\ 2,\ 2,\ 7,\ 5,\ 7\}$

(2) **Providing a property:** $\{x \mid P(x)\}$

$C = \{x \mid x$ **is a prime**$\}$,

$D = \{x \mid x$ **is an English word and** x **is a palindrome**$\}$,

$E = \{x \mid x$ **is a positive integer divisible by 3 and less than 10** $\}$

(3) **Recursively defined:**

General form:

i) **Certain initial or base elements in** A

ii) **If** $a,\ b \in A$, **then** $a \circ b \in A$

iii) **No other elements belong to** A

Example Defining A:

i) $7 \in A$

ii) If $a,\ b \in A$, then $a + b \in A$

iii) No other elements belong to A

(4) **Closure defined**

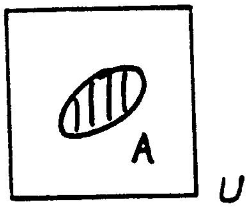
- We say that a set $\underline{A}$ is closed under a binary operation $\underline{\circ}$ if for all $\underline{a,\ b \in A}$, $\underline{a \circ b \in A}$
- Let $B \supseteq A$ and B be closed under $\circ$. We say that B is a closure of A with respect to $\circ$ if there is no B' such that $A \subseteq B' \subset B$ and B' is closed under $\circ$.
- General form (for closure defined sets)
  A is the smallest set containing certain initial or base elements that is closed under an operation $\circ$.

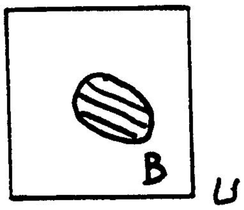
Example

B is the smallest set containing 7
that is closed under "+".

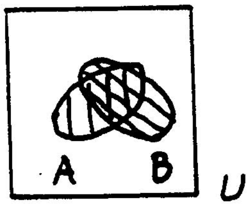
— **<u>Set operations</u>**

Given A and B two sets:

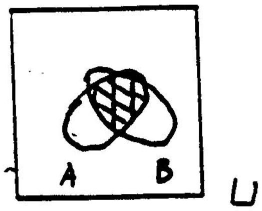




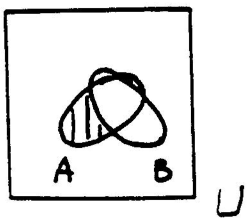
$A \cup B = \{x \mid x$ **is in** A **or** x **is in** $B\}$



$A \cap B = \{x \mid x$ **is in** A **and** x **is in** $B\}$



$A - B = \{x \mid x$ **is in** A **and** x **is not in** $B\}$



$\cup_{i=1}^{n} A_i = \{x \mid x \textbf{ is in } A_i,\ \textbf{for some } i,\ 1 \leq i \leq n\}$
$\cap_{i=1}^{n} A_i = \{x \mid x \textbf{ is in } A_i,\ 1 \leq i \leq n\}$

— **Properties of set operations**

Distributivity

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

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

Indempotence

$A \cup A = A;\ A \cap A = A$

Involution

$\neg(\neg A) = A$

Commutativity

$A \cap B = B \cap A;\ A \cup B = B \cup A$

Associativity

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

$A \cap (B \cap C) = (A \cap B) \cap C$

De Morgan's rules

$\neg(A \cup B) = \neg A \cap \neg B$

$\neg(A \cap B) = \neg A \cup \neg B$

— **Power set**

The collection of all subsets of A is called the power set of A, and is denoted by 2^A.

Example:

$A = \{2, 3, 5\}$

$2^A = \{\emptyset, \{2\}, \{3\}, \{5\}, \{2, 3\}, \{2, 5\}, \{3, 5\}, \{2, 3, 5\}\}$

— **Some special sets:**

$\emptyset$**: the empty set;**

$\mathcal{Z}$**: the set of all integers;**

$\mathcal{N}$**: the set of all positive integers;**

$\mathcal{N}_0$**: the set of all nonnegative integers;**

$\mathcal{R}$**: the set of all real numbers.**

. . . .

2. Multisets

A multiset is a collection of elements from some universe, in which repetitions are not ignored.

3. Sequences

A sequence of elements, from some universe, is a list of elements which are ordered by position.

4. Functions

Definition Given two sets A and B, a (partial) function from A into B associates with each a in A (at most) one element b of B.

Notations:

function $f : A \rightarrow B$

association $f(a) = b$

undefined $f(a) = undef$

Special functions:

identity function:

$f : A \rightarrow A$ **and**

$f(a) = a$ **for all** $a \in A$

Characteristic function of A for B:

$B \subseteq A$

$f : A \rightarrow \{true,\ false\}$

$f(a) = true,\ if\ a \in B$

$f(a) = false,\ if\ a \in A - B$

Some properties of functions $f : A \rightarrow B$

total:

f(a) is defined for all a **in** A

surjective (onto):

for all b **in** B **there is an** a **in** A **such that** $f(a) = b$

injective (one-to-one):

$a,\ a' \in A,\ a \neq a'$ **implies that** $f(a) \neq f(a')$

bijective (one-to-one onto):

both surjective and injective

Big-O Notation

$f(n) = O(g(n))$ **if there are a positive integer** c **and a positive integer** d **such that for all** $n \geq d$

$$f(n) \leq cg(n)$$

$f(n) = \Omega(g(n))$ **if**

$$cf(n) \geq g(n)$$

$f(n) = \Theta(g(n))$ **if**

$$f(n) = O(g(n)) \text{ and } f(n) = \Omega(g(n))$$

m,n-place (partial) function

$$f : A_1 \times A_2 \times \ldots \times A_m \to B_1 \times \ldots \times B_n$$

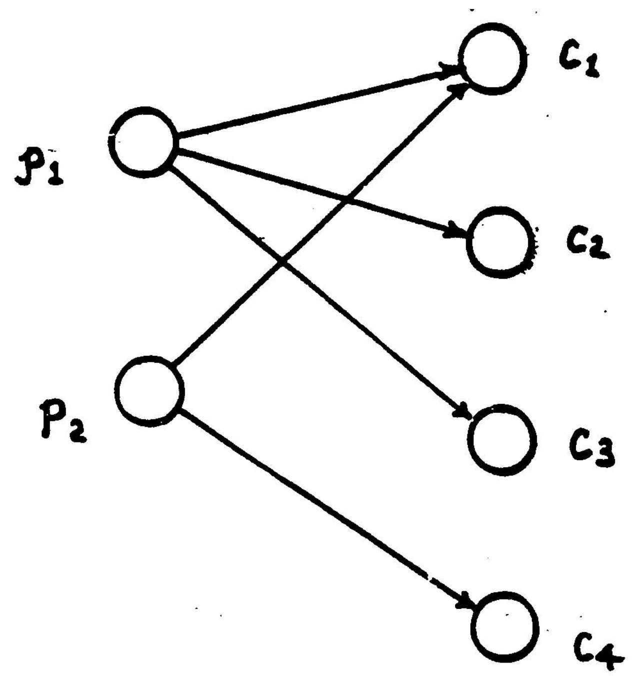
$$f(a_1, a_2, \ldots, a_m) = (b_1, \ldots, b_n)$$

$$\textbf{or}\;\; f(a_1, a_2, \ldots, a_m) = undef$$

5. Relations

An n-ary relation R, $n \geq 1$, with respect to the sets $A_1, \ldots, A_n$ is any subset R of $A_1 \times \ldots \times A_n$.

Example



$$P = \{p_1, p_2\},\ C = \{c_1, c_2, c_3, c_4\}$$
$$T \subseteq P \times C$$
$$T = \{(p_1, c_1), (p_1, c_2), (p_1, c_3), (p_2, c_1), (p_2, c_4)\}$$

Composition of relations

Let $R \subseteq A \times B$ **and** $S \subseteq B \times C$ **be two relations. Then the composition of** R **with** S**, denoted by** $R \circ S$**, is the relation** $R \circ S \subseteq A \times C$**, defined by:**

$$R \circ S = \{(a,c) \mid (a,b) \textbf{ is in } R \textbf{ and } (b,c) \textbf{ is in } S \textbf{ for some } b \textbf{ in } B\}$$

Composition of relation $R : A \times A$ with itself

$R^0 \;:\; \{(a,a) \mid a \textbf{ is in } A\}$

$R^1 \;:\; R$

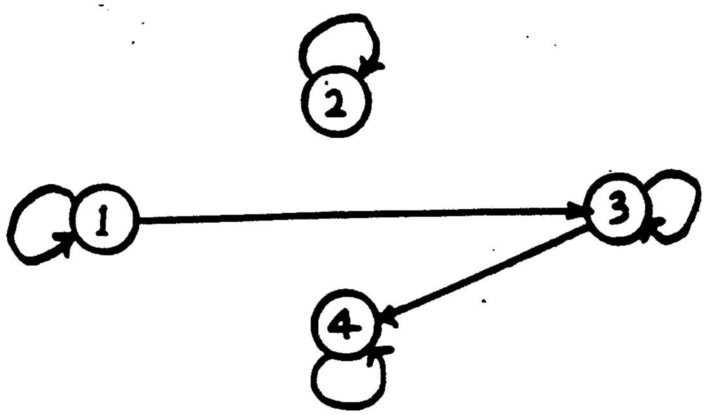
$R^i,\ {}_{i>1} \;:\; R \circ R^{i-1}$

$R^+ = \cup_{i=1}^{\infty} R^i$ **transitive closure of** R

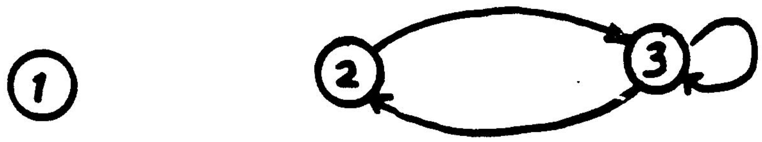
$R^* = \cup_{i=0}^{\infty} R^i$ **reflexive transitive closure of** R

Properties of relation $R \subseteq A \times A$

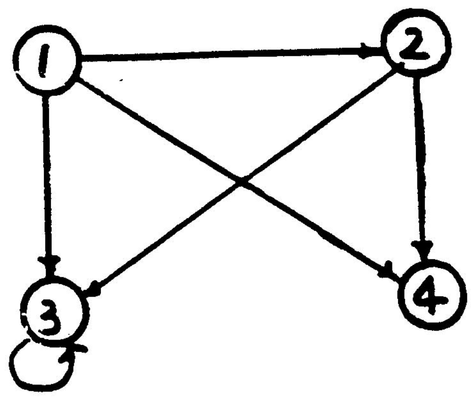
- **reflexive:** aRa **for all** a **in** A



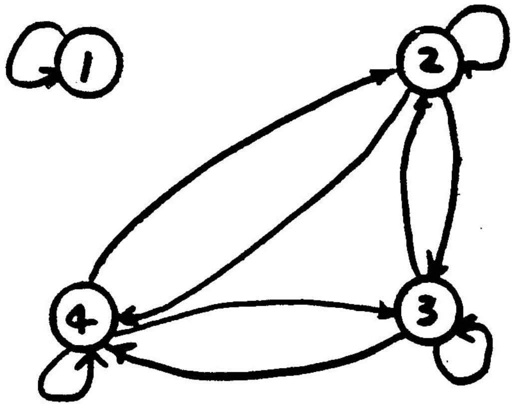
- **symmetric:** aRb **implies** bRa



- **antisymmetric:** $aRb,\ bRa$ **implies** $a = b$



- **transitive:** $aRb,\ bRc$ **implies** aRc



△ **A binary relation** R **over** A **is an equivalence relation if it is**

- **reflexive,**
- **symmetric, and**
- **transitive.**

△ **An equivalence relation** R **over** A **defines disjoint subsets of** A**, called equivalence classes.**

$$[a]_R = \{b \mid b \textbf{ is in } A \textbf{ and } aRb\}$$

- **Let R be a binary relation over A and $B \subseteq A$. We say that B is <u>R-closed</u> if for all a in B, aRb implies that b is in B.**

  <u>Example</u> A : **set of all integers;**
  $B = \{9, 4, 3, 2\}$**;**
  R :**"is the square of"**
  Then B is R-closed.

- R **is an <u>n-ary</u> relation over A. $B \subseteq A$ is <u>R-closed</u> if for all $b_1, \ldots, b_{n-1}$ in B,** $(b_1, \ldots, b_{n-1}, b_n)$ **is in R implies b_n is in B.**

  <u>Example</u> A : **set of all integers;**
  $R = \{(a, b, c) \mid a \times b = c\}$**;**
  $B = \{ia \mid i \geq 1\}$ **for some integer** a
  Then B is R-closed.

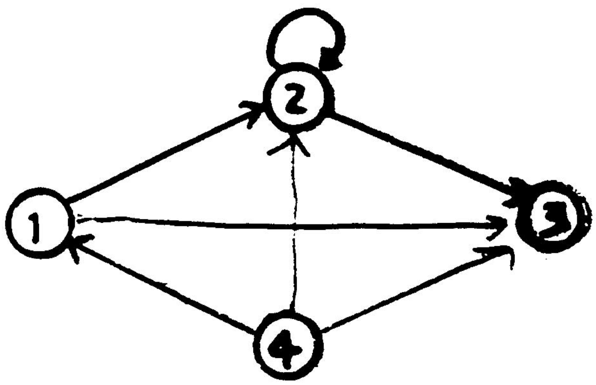
Lemma Let R be an equivalence relation over A. Then for all a, b in A either $[a]_R = [b]_R$ or $[a]_R \cap [b]_R = \emptyset$

△ **A binary relation R over A is a partial order if it is**

- **reflexive,**
- **transitive, and**
- **antisymmetric.**

△ **Closure**

- R^+ **is the transitive closure of** R
- **Digraph representation of a transitive closure:**



6. Cardinality

△ **Given two sets A and B, we say that they have equal cardinality if there is a bijection $f : A \rightarrow B$.**

Example $\#\mathcal{Z} = \#\mathcal{N}_0$

$f(i) = -2i - 1, \ i < 0$

$f(i) = 2i, \ i \geq 0$

△ **A set is countable or enumerable if either it is finite or it is infinite and has equal cardinality with $\mathcal{N}$.**

7. Proof Methods

— direct proof
— proof by contradiction
— proof by induction

△ **Direct proof**

We enumerate all cases to show that something does hold.

Example **Every even number between 4 and 2^{32} is a sum of two primes.**

△ **Proof by contradiction**

We establish the validity of a claim by assuming it does not hold and inferring a contradiction.

Example **There are an infinite number of primes.**

$\triangle$ **<u>Proof by induction</u>**

– **basis**

– **induction hypothesis**

– **induction step**

Two forms:

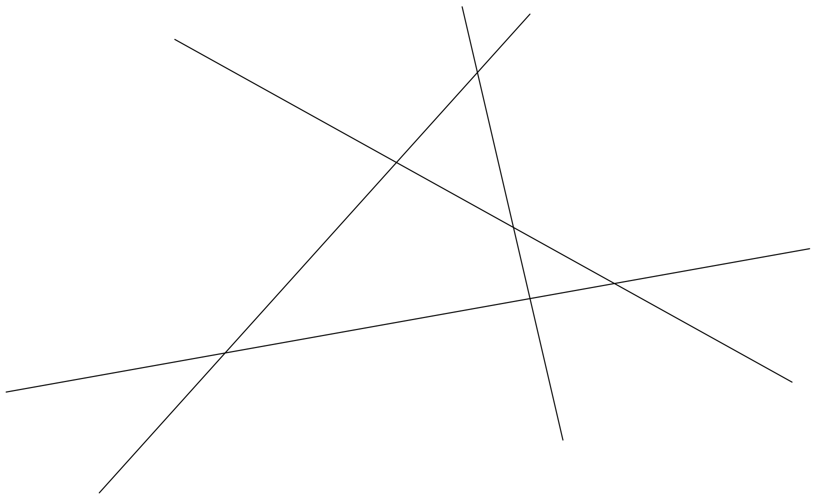
(1) — Prove it holds for a basis value b,
— Hypothesize it holds for value n,
— Prove it holds for value $n+1$.

(2) — Prove it holds for basis values,
— Hypothesize it holds for all values less than n and greater than basis value,
— Prove it holds for value n.

Example (proof by induction)

(i) no two lines are parallel;

(ii) no three lines have a common intersection point.



Prove that the number of regions in an arrangement of n lines is

$$1 + n(n + 1)/2$$

8. Proof Techniques

— **pigeonhole principle**

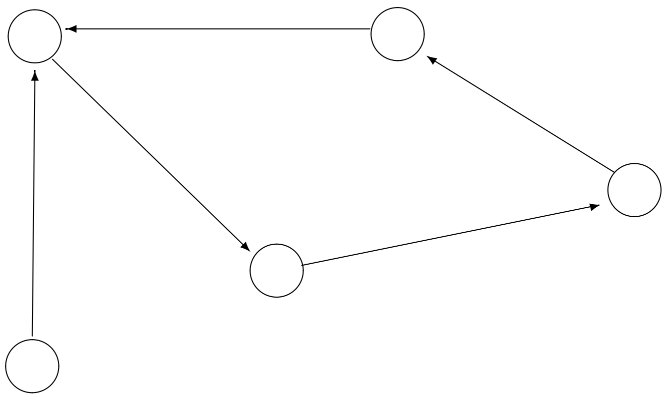
— **counting**

— **diagonalisation**

The Pigeonhole Principle
Let $n \geq 1$ **be an integer, let there be** n **pigeonholes, and there be** $n+1$ **items of mail to be placed in the pigeonholes. Then, however the the items are placed, at least one pigeonhole will contain at least two items.**

The Pigeonhole Principle(Extended version)
Let $q_1, \ldots, q_t \geq 1$**. There exists a positive integer** $N(q_1, \ldots, q_t)$**. If** $n \geq N(q_1, \ldots, q_t)$**, then however** n **items are placed into** t **pigeonholes, there exists** i, $1 \leq i \leq t$ **such that the** i**-th pigeonhole contains at least** $q_i + 1$ **items.**

<u>Example</u> Let $G = (V, E)$ be a digraph with $\#V = n \geq 1$. Then G has a cycle if and only if G has a path of length at least n.



9. Alphabets, Words, and Languages

△ **An alphabet is a finite, nonempty set of elements.**
The elements of the alphabet are called symbols or letters.

△ **A word over an alphabet Σ is a finite sequence of symbols from Σ.**

△ **A language is a set of words.**

Examples:

(1) English alphabet, words and language.

(2) Alphabet: $\{a,\ b\}$
words: $\varepsilon, a,\ b,\ ab,\ ba,\ \ldots\ldots$
language: $\{\varepsilon,\ ab,\ aabb,\ aaabbb,\ \ldots\ldots\}$
i.e. $\{a^i b^i \mid i \geq 0\}$

(3) Alphabet : Fortran reserved words and identifiers

words : a Fortran program

Language : the set of all Fortran programs.

△ **Empty word is a word over every alphabet.**

$$\varepsilon$$

△ **The length of a word is the number of symbols in the given word.**

Example:

$$|\varepsilon| = 0$$

$$|abbc| = 4$$

△ **The a-length of a word x is the number of times a occurs in x.**

Example:

$$|01101|_0 = 2$$

$$|cbcbc|_a = 0$$

△ **The <u>catenation</u> of two words x and y, denoted by xy, is the word obtained by appending the word y to x.**

<u>Example</u> $$\begin{aligned} x &= abc \\ y &= defg \\ xy &= abcdefg \\ yx &= defgabc \end{aligned}$$

$$x\varepsilon = \varepsilon x = x$$

$$\varepsilon\varepsilon = \varepsilon$$

△ **Catenation is <u>associative</u>:**

$$(xy)z = x(yz)$$

△ $|xy| = |x| + |y|$

$\triangle$ $x^0 = \varepsilon$ **(Power of a word)**

$x^i = xx^{i-1},\ i \geq 1$

Example $(abc)^0 = \varepsilon$

$(abc)^3 = abcabcabc$

$\triangle$ **Prefix:** x **is a prefix of** y **if** $\exists z$ **such that**

$$xz = y$$

Example
- *not* **is a prefix of** *notice*
- ε **is a prefix of any word**
- **Any word is a prefix of itself**

$\triangle$ **Suffix:** x **is a suffix of** y **if** $\exists z$ **such that**

$$zx = y$$

Example
- *allow* **is a suffix of** *swallow*
- ε **is a suffix of any word**
- 01011 **is a suffix of** 01011

$\triangle$ **Subword:** x **is a subword of** y **if** $\exists w, z$ **s.t.**

$$wxz = y$$

Example **The subwords of** $\underline{beat}$ **are:**

$$\varepsilon,\ b,\ e,\ a,\ t,\ be,\ ea,\ at,\ bea,\ eat,\ beat$$

$\triangle$ **Proper prefix (suffix, subword):**

x **is a proper prefix (suffix, subword) of** y **if** x **is a prefix (suffix, subword) of** y **and** $x \neq \varepsilon$ **and** $x \neq y$**.**

$\triangle$ **<u>Reversal</u>:**

(i) $x^R = x$, **if** $x = \varepsilon$**;**

(ii) $x^R = y^R a$, **if** $x = ay$ **for** $a \in \Sigma$, y **is a word**

<u>Lemma</u> If $x = a_1 \dots a_n$ **for some** $n \geq 0$, **then**

$$x^R = a_n \dots a_1.$$

<u>Proof:</u> By induction on $|x|$**.**

<u>Basis</u>: $|x| = 0$. $\varepsilon^R = \varepsilon$ **by (i).**

<u>I.H.</u>: Assume Lemma holds for all x **with** $|x| = n$**.**

<u>I.S.</u>: Consider a word x **with** $|x| = n + 1$**.**

Then $x = a_1 \dots a_{n+1} = a_1 u$, **where**

$$u = a_2 \dots a_{n+1}.$$

Then $x^R = u^R a_1$**.**

But $|u| = n$, **by I.H.,** $u^R = a_{n+1} \dots a_2$,

so we get

$$x^R = a_{n+1} \dots a_1. \ qed$$

$\triangle$ **Universal Language over** Σ**:** Σ^*

$\Sigma = \{0, 1\}$, $\Sigma^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \dots\}$

$\triangle$ Mappings (<u>Morphism</u> and <u>Substitution</u>)

<u>Definition</u> Let Σ and Δ be two alphabets. Then a mapping $h : \Sigma^* \to \Delta^*$ is said to be a <u>morphism</u> if

(i) $h(\varepsilon) = \varepsilon$**;**

(ii) $h(xy) = h(x)h(y)$**, for all** $x,\ y$ **in** Σ^***.**

<u>Note</u>: (ii) implies that we need only define the images of letters to define the images of words.

<u>Example</u>:

$\Sigma = \{0,\ 1\}, \quad \Delta = \{a,\ b,\ c,\ d\},$

$h(0) = baac, \quad h(1) = \varepsilon.$

Then $h(1001) = h(1)h(0)h(0)h(1) = \varepsilon baacbaac\varepsilon = baacbaac$

A morphism h **is said to be** ε**-free if, for all** $x \neq \varepsilon, \quad h(x) \neq \varepsilon.$

Definition Let Σ and Δ be two alphabets. A mapping $\sigma : \Sigma^* \to 2^{\Delta^*}$ is said to be a substitution if

i) $\sigma(\varepsilon) = \{\varepsilon\}$;

ii) $\sigma(xy) = \sigma(x)\sigma(y)$, for all $x,\ y \in \Sigma^*$.

Example:

$\Sigma_1 = \{a,\ b\}, \quad \Delta_1 = \{a,\ b,\ c\}$,

a substitution σ_1:

$\sigma_1(a) = \{ab,\ ac,\ b\}$; $\sigma_1(b) = \{b,\ ba\}$.

Then $\sigma_1(ba) =$

Example:

$\Sigma_2 = \{0,\ 1,\ 2\}, \quad \Delta_2 = \{a,\ b\}$,

$\sigma_2(0) = \{a^i \mid i \geq 1\}$

$\sigma_2(1) = \{b^i \mid i \geq 1\}$

$\sigma_2(2) = \{\varepsilon\}$

Then $\sigma_2(1020) =$

$\triangle$ **Given an alphabet** Σ, Σ^* **is defined as follows:**

(i) $\varepsilon \in \Sigma^*$**;**

(ii) if $x \in \Sigma^*$, **then** $ax \in \Sigma^*$ **for all** $a \in \Sigma$**.**

$\triangle$ **A language** L **over an alphabet** Σ **is a subset of** Σ^***, i.e.,** $L \subseteq \Sigma^*$**.**

Example:

ϕ **is a language over every alphabet .**

$\{\varepsilon\}$ **is a language over every alphabet.**

$\{a^i b^i \mid i \geq 0\}$ **is a language over** $\{a,\ b\}$

$\{a^i b^i c^i \mid i \geq 0\}$ **is a language over** $\{a,\ b,\ c\}$

$\triangle$ <u>Catenation</u> of Languages

$L_1 \circ L_2 = \{x_1 \circ x_2 \mid x_1$ **in** $L_1,\ x_2$ **in** $L_2\}$**,**
usually written as $L_1 L_2$**.**

<u>Examples</u>

$L_1 = \{a,\ ab\}; \quad L_2 = \{bc,\ c\}$

$L_1 L_2 = \{abc,\ ac,\ abbc\}$

(Note that $L_1 \times L_2 = \{(a, bc), (a, c), (ab, bc), (ab, c)\}$**)**

$\phi L_1 =$

$\{\varepsilon\} L_1 =$

$\{\varepsilon\} \phi =$

$L_A = \{a,\ \varepsilon\}; \qquad L_B = \{ab,\ b\}$

$L_A L_B =$

$\triangle$ **Powers of Languages:**

$$L^0 = \{\varepsilon\}$$

$$L^{n+1} = L^n \circ L,\ \ n \geq 1$$

$\triangle$ **Plus**

$$L^+ = \cup_{i=1}^{\infty} L^i$$

$\triangle$ **Star**

$$L^* = \cup_{i=0}^{\infty} L^i \qquad\qquad L^0 \cup L^1 \cup L^2 \cup \ldots\ldots$$

Examples

$L = \{ab,\ b\}$. **Then**

$$L^0 = \{\varepsilon\}$$

$$L^1 = L = \{ab,\ b\}$$

$$L^2 = \{abab,\ bab,\ abb,\ bb\}$$

$$\phi^0 = \{\varepsilon\} \neq \phi$$

$$\{\varepsilon\}^0 = \{\varepsilon\}$$

$$L^* = \{\varepsilon,\ ab,\ b,\ abab,\ bab,\ abb,\ bb,\ \ldots\ldots\}$$

(**Note** $abababab \in L^4$)

△ **<u>Reversal of Languages</u>**

$L^R = \{x^R \mid x$ **is in** $L\}$

<u>Examples</u>

$L_F = \{aab,\ abb,\ abbb\}$**;**

$L_F^R = \{baa,\ bba,\ bbba\}$

$L_I = \{a^m b^n \mid m > n > 0\}$

$L_I^R = \{b^n a^m \mid m > n > 0\}$

— **Properties of <u>reversal</u>**

$$\begin{aligned}(A \cup B)^R &= A^R \cup B^R\\ (A \cap B)^R &= A^R \cap B^R\\ (AB)^R &= B^R A^R\\ (A^+)^R &= (A^R)^+\\ (A^*)^R &= (A^R)^*\end{aligned}$$

△ **<u>Complementation</u> of Languages**

Given a language L **over** Σ**,**

$\overline{L} = \Sigma^* - L$

$\overline{\Sigma^*} = \phi$ $\qquad$ $\overline{\Sigma^+} = \{\varepsilon\}$ $\qquad$ $(\overline{A})^R = \overline{A^R}$

$L = \{a^n b^n \mid n \geq 0\}$ **over** $\Sigma = \{a,\ b\}$

$\overline{L} =$

△ <u>**Alternative definition of L^+ and L^***</u>

$$L^+ = \{w \textbf{ in } \Sigma^* \mid w = w_1 w_2 \ldots w_n, \textbf{ for } w_1, w_2, \ldots, w_n \in L \textbf{ and } \underline{n \geq 1}\}$$

$$L^* = \{w \textbf{ in } \Sigma^* \mid w = w_1 w_2 \ldots w_n, \textbf{ for } w_1, w_2, \ldots, w_n \in L \textbf{ and } \underline{n \geq 0}\}$$

△ **Given a word x in Σ^*, and a language $L \subseteq \Sigma^*$ to test if x is in L^* we use $L^* = \cup_{i=0}^{\infty} L^i$ and test if x is in L^0, L^1, ...**

△ <u>**Property Summaries**</u>

— **properties of <u>catenation</u> (of languages)**

Associativity — $L_1(L_2L_3) = (L_1L_2)L_3$

Identity — $L\{\varepsilon\} = \{\varepsilon\}L = L$

Zero — $L\phi = \phi L = \phi$

Distributivity — $L_1(L_2 \cup L_3) = L_1L_2 \cup L_1L_3$

w.r.t. $\cup$ $\quad (L_1 \cup L_2)L_3 = L_1L_3 \cup L_2L_3$

Distributivity does <u>not hold</u> with respect to $\cap$

— **properties of <u>Plus</u> and <u>Star</u>**

$$
\begin{aligned}
L^* &= L^+ \cup \{\varepsilon\} \quad (\textbf{ But } L^+ = L^* - \{\varepsilon\}?) \\
L^+ &= LL^* \\
(L^+)^+ &= L^+, \quad (L^*)^* = L^* \\
\phi^+ &= \phi, \qquad \phi^* = \{\varepsilon\}, \quad \phi^0 = \{\varepsilon\} \\
\{\varepsilon\}^+ &= \{\varepsilon\}, \quad \{\varepsilon\}^* = \{\varepsilon\}, \quad \phi^2 = \phi \\
L^+L &= LL^+, \quad L^*L = LL^* \\
A \subseteq B &\Rightarrow A^+ \subseteq B^+ \textbf{ and } A^* \subseteq B^*
\end{aligned}
$$