771 Η - Θεωρία Υπολογισμών και Αλγορίθμων

Σημειώσεις – Μέρος 1ο

Διδάσκων: Α. Ντελόπουλος

Το παρόν αποτελεί σημειώσεις που αντιστοιχούν σε μέρος των διαλέξεων για το μάθημα **771 Η - Θεωρία Υπολογισμών και Αλγορίθμων** του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Αριστοτέλειου Πανεπιστήμιου Θεσσαλονίκης.

Το υλικό των διαλέξεων και των σημειώσεων στηρίζεται σε μεγάλο βαθμό στην ύλη του βιβλίου: *Harry R. Lewis and Christos H. Papadimitriou, "Elements of the Theory of Computation," 2nd edition, Prentice Hall, 1998.*

Σύνολα – Σχέσεις – Συναρτήσεις – Αλγόριθμοι – Γλώσσες

Ορισμοί, Ιδιότητες

Σύνολα – ορισμός, αναπαράσταση

- Σύνολο: ‘συλλογή αντικειμένων’
- *Παραδείγματα:*
  - *A = {a, b, c} = {a, c, b}*
  - *A = {1, {x,y}, x, y, z}*
  - *A = {x/x έχει την ιδιότητα P}*
    - *A ={x/x είναι θετικός ακέραιος >18} = {19,20,21,...}*
- |A| = ‘το πλήθος των στοιχείων του A’ *(πληθικός αριθμός)*

Σύνολα – βασικές πράξεις

$$A \bigcup B = \{x / x \in A \;\; OR \;\; x \in B\}$$

$$A \bigcap B = \{x / x \in A \;\; AND \;\; x \in B\}$$

$$A - B = \{x / x \in A \;\; AND \;\; x \notin B\}$$

2^A = {το σύνολο με στοιχεία όλα τα υποσύνολα του A}

π.χ., $2^{\{a,b\}} = \{\{a,b\},\{a\},\{b\},\varnothing\}$

Σύνολα – ιδιότητες βασικών πράξεων

$A \bigcup A = A$

$A \bigcap A = A$

$A \bigcup B = B \bigcup A$ (μεταθετική)

$A \bigcap B = B \bigcap A$

$(A \bigcup B) \bigcup C = A \bigcup (B \bigcup C)$ (προσεταιριστική)

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

$(A \bigcup B) \bigcap C = (A \bigcap C) \bigcup (B \bigcap C)$ (επιμεριστική)

$(A \bigcap B) \bigcup C = (A \bigcup C) \bigcap (B \bigcup C)$

$(A \bigcup B) \bigcap A = A$

$(A \bigcap B) \bigcup A = A$

$A - (B \bigcup C) = (A - B) \bigcap (A - C)$ $(De'Morgan)$

$A - (B \bigcap C) = (A - B) \bigcup (A - C)$

Σύνολα – διαμερίσεις

•Βοηθητικοί ορισμοί

$\bigcup S \equiv \{x \,/\, \exists A \in S : x \in A\}$

$\bigcap S \equiv \{x \,/\, \forall A \in S : x \in A\}$

π.χ.
$S = \{\{a,b\},\{b,c\},\{b,d\}\}$

$\bigcup S \equiv \{a,b,c,d\} \qquad \bigcap S \equiv \{b\}$

•Το Π *είναι* ***διαμέριση*** του *A* όταν:

$$\Pi \subseteq 2^A$$

$$\varnothing \notin \Pi$$

$$K, L \in \Pi \Rightarrow K \bigcap L = \varnothing$$

$$\bigcup \Pi = A$$

Σχέσεις και Συναρτήσεις

- Διατεταγμένο ζεύγος:

$$(a,b) \neq (b,a)$$

$$"(a,b) = (c,d)" \Leftrightarrow "a = c \quad AND \quad b = d"$$

- Διατεταγμένη n-άδα: $(a_1, a_2, \ldots, a_n)$
- ***Καρτεσιανό γινόμενο***:

$$A_1 \times A_2 \times \ldots \times A_n \equiv \{(x_1, x_2, \ldots, x_n) \,/\, x_i \in A_i, i = 1, \ldots, n\}$$

π.χ. $\{a,b\} \times \{0,1,2\} \equiv \{(a,0),(a,1),(a,2),(b,0),(b,1),(b,2)\}$

Σχέσεις

- Διαδική σχέση, *R,* στα *A, B* (με αυτή τη σειρά!):
  - οποιοδήποτε υποσύνολο *R* του *A x B*
- n-πλή σχέση, *R*, στα $A_1, A_2, ..., A_n$ (με αυτή τη σειρά!):
  - οποιοδήποτε υποσύνολο *R* του A_1 x A_2 x...x A_n
- Αντίστροφη σχέση της *R*:
  - $R^{-1} = \{ (y,x) / (x,y) \in R \} \subseteq B \times A$

Συναρτήσεις

- ***Συνάρτηση f*** από το *A* στο *B*:
  - Γράφουμε $f : A \to B$
- Ορισμός: Η *f* είναι οποιαδήποτε *διαδική σχέση* τέτοια ώστε: $\forall a \in A \ \ \exists_1^1 (a,b) \in f \qquad (\ \exists_1^1 : \ \text{"}\exists \ 1 \ \text{και} \ \ \text{μόνο} \ \ 1\text{"} \ )$
- Πεδίο ορισμού: *A*
- Πεδίο τιμών: $f(A)=\{b / b \in B \text{ και } \exists \, (a,b) \in f \}$
- Προβολή του $A_1 \subseteq A$:

$$f(A_1)=\{b / b \in B \text{ και } \exists \, (a,b) \in f \text{ με } a \in A_1\}$$

Συναρτήσεις ‘πολλών μεταβλητών’

- f: $A_1 \times A_2 \times \ldots \times A_n \rightarrow B$
- *Γράφουμε:* $f(a_1, a_2, \ldots, a_n) = b$
- $a_1, a_2, \ldots, a_n$ *: ορίσματα*
- *b: τιμή*

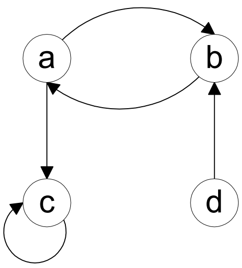
Ειδικές Συναρτήσεις

- “ένα προς ένα” (1-1)
  - “ $a_1 \neq a_2$ συνεπάγεται $f(a_1) \neq f(a_2)$ ”
- “επί”
  - “ f(A) = B ”
- αντιστοιχία (bijection)
  - “1-1” και “επί” ($f^{-1}(f(A)) = A$)

Ειδικοί τύποι διαδικών σχέσεων

$$R \subseteq A \times A$$

Δέχονται αναπαραστάσεις μέσω κατευθυντικών γράφων



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

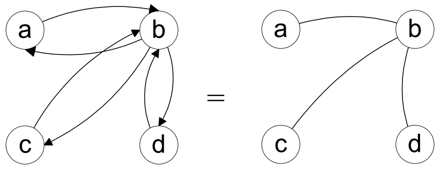
Μονοπάτι $(a_1, a_2, .., a_n)$
μήκους n: $(a_i, a_{i+1}) \in R$

Ειδικοί τύποι διαδικών σχέσεων – Ιδιότητες

ανακλαστική σχέση: $(a,a) \in R, \quad \forall a \in A$

συμμετρική σχέση: $(a,b) \in R \Rightarrow (b,a) \in R$

Οι συμμετρικές σχέσεις αναπαρίστανται με **μή** κατευθυντικούς γράφους



Ειδικοί τύποι διαδικών σχέσεων – Ιδιότητες

αντισυμμετρική σχέση: $(a,b) \in R \;\;\&\;\; a \neq b \Rightarrow (b,a) \notin R$

μεταβατική σχέση: $(a,b) \in R \;\;\&\;\; (b,c) \in R \Rightarrow (a,c) \in R$

σχέση ισοδυναμίας:

ανακλαστική & συμμετρική & μεταβατική

σχέση μερικής διαμέρισης:

ανακλαστική & **αντι**συμμετρική & μεταβατική

σχέση ολικής διαμέρισης:

μερική διαμέριση & $\forall a,b \in A \Rightarrow (a,b) \in R \;\; ή \;\; (b,\alpha) \in R$

Ιδιότητες σχέσεων ισοδυναμίας

κλάση ισοδυναμίας [a]:

Το υποσύνολο των στοιχείων του Α που σχετίζονται (είναι ισοδύναμα) με το a∈ Α

Θεώρημα: Αν η R είναι σχέση ισοδυναμίας στο Α≠∅ τότε το **σύνολο των κλάσεων ισοδυναμίας** της, Π, αποτελεί **διαμέριση** του Α.

Απόδειξη: *Δείχνουμε ότι:*

$$\begin{array}{|l|}\hline \Pi \subseteq 2^{A} \\ \varnothing \notin \Pi \\ K, L \in \Pi \Rightarrow K \cap L = \varnothing \\ \bigcup \Pi = A \\ \hline \end{array}$$

Πεπερασμένα σύνολα και απειροσύνολα

τα σύνολα A,B είναι **ισοπληθή** όταν:

- υπάρχει *αντιστοιχία* f: $A \rightarrow B$

το σύνολο A είναι **πεπερασμένο**:

- υπάρχει *αντιστοιχία* f: $A \rightarrow \{1,2,3,...,n\}$ για κάποιο $n \in N$ (N=φυσικοί αριθμοί)
- τότε $|A| = n$

το σύνολο A είναι **απειροσύνολο**: δεν είναι πεπερασμένο

το απειροσύνολο A είναι **μετρήσιμο**:

- Υπάρχει *αντιστοιχία* f: $A \rightarrow N$
  - δηλ. υπάρχει τρόπος απαρίθμησης των στοιχείων του A
  - η μέθοδος της πλακόστρωσης

Τρείς μέθοδοι απόδειξης - 1

- Η αρχή της **μαθηματικής επαγωγής**
  - αν $0 \in A$ και $\{0,1,2,...,n\} \subseteq A$ τότε $n+1 \in A$
  - πρακτικά τη χρησιμοποιούμε για A={n / 'η πρόταση P είναι αληθής για τον αριθμό n'}
    - δείχνουμε ότι $0 \in A$ (δηλ. η P αληθεύει για το 0)
    - υποθέτουμε ότι $\{0,1,2,...,n\} \subseteq A$ (δηλ. ότι η P αληθεύει για 0,1,…,n)
    - με βάση τα παραπάνω αποδεικνύουμε ότι και το $n+1 \in A$ (δηλ. η P αληθεύει για το n+1)

Τρείς μέθοδοι απόδειξης - 2

- Η αρχή της **φωλιάς των περιστεριών**
  - αν τα σύνολα A και B είναι πεπερασμένα και |A|> |B| τότε **δεν υπάρχει "1-1"** f:A→B
  - δηλ. αν A είναι τα περιστέρια και B οι φωλιές, σε κάποια φωλιά θα κοιμηθούν περισσότερα του ενός περιστέρια.
  - Απόδειξη: με τη μέθοδο της επαγωγής

Τρείς μέθοδοι απόδειξης - 3

- Η αρχή της **διαγωνιοποίησης**
  - Εστω:
    - R διαδική σχέση στο σύνολο A
    - D = {a : a $\in$ A και (a,a) $\notin$ R} ("διαγώνιο σύνολο της R στο A")
    - R_a = {b : b $\in$ A και (a,b) $\in$ R}, για κάθε a $\in$ A
  - Τότε: το D είναι ***διαφορετικό*** από κάθε R_a
  - Επίδειξη:

R	a	b	c	d	e	f	
a	o	x		x			R_a = {b,d}
b		x	x				R_b = {b,c}
c			x				R_c = {c}
d		x	x	o	x	x	R_d = {b,c,e,f}
e					x	x	R_e = {e,f}
f	x		x	x	x	o	R_f = {a,c,d,e}

D_c = {b,c,e} D={a,d,f}

Κλειστότητα και Ιδιότητες Κλειστότητας

Ορισμοί:

1. Έστω: σύνολο D, $n \geq 0$, σχέση $R \subseteq D^{n+1}$, $B \subseteq D$

   Τότε: B **κλειστό** ως προς την R όταν:

   '$b_1, b_2, \ldots, b_n \in B$ και $(b_1, b_2, \ldots, b_n, b_{n+1}) \in R$' $\Rightarrow$ $b_{n+1} \in B$

2. Κάθε ιδιότητα του τύπου 'το B είναι κλειστό ώς προς τις σχέσεις $R_1, R_2, \ldots, R_m$' λέγεται **ιδιότητα κλειστότητας**

Παραδείγματα Κλειστότητας

#1: "ο πρόγονος του πρόγονου είναι πρόγονος"

- B={x/x πρόγονος του *Νίκου*}$\subseteq$D={άνθρωποι}
- R={(a,b): b γονιός του a}
- Τότε το B είναι κλειστό ως προς την R
- Απόδειξη: Αν $a \in B$ και $(a,b) \in R \Rightarrow$ b γονιός του a $\Rightarrow$ b πρόγονος του a $\Rightarrow$ b πρόγονος του *Νίκου* (γιατί;)

#2: "*Και οι σχέσεις είναι σύνολα!*"

- $B=R_o$ σχέση στο A ($R_o \subseteq D=A \times A$)
- $R=\{((a,b),(b,c),(a,c)): a,b,c \in A\}$
- Η R_o είναι κλειστή ως προς την R *αν και μόνο αν* η R_o είναι **μεταβατική**!

  (Αποδείξτε το!)

‘Κλείσιμο’ συνόλων

- Θεώρημα: Έστω (1) P ιδιότητα κλειστότητας από τις σχέσεις $R_1,\ldots,R_m$ σε σύνολο D και (2) $A \subseteq D$. Τότε *υπάρχει μοναδικό* **ελάχιστο σύνολο** $B \supseteq A$ με την ιδιότητα P (δηλ. *κλειστό* ως προς $R_1,\ldots,R_m$).

(*ελάχιστο σύνολο : ΔΕΝ ∃ B’ ⊆ B με τις δύο παραπάνω ιδιότητες δηλ.* $B' \supseteq A$ και P)

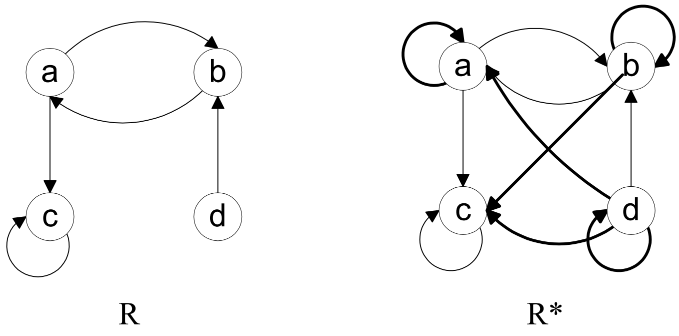
- Μάλιστα $B = \bigcap S$ όπου $S=\{B_i / \text{“}A \subseteq B_i \subseteq D\text{”}$ **και** “B_i κλειστό ως προς $R_1,\ldots,R_m$(δηλ. B_i έχει την ιδιότητα P)”}
- Ορισμός: Το παραπάνω (ελάχιστο) B λέγεται **κλείσιμο** του A ως προς την ιδιότητα κλειστότητας P (ή ισοδύναμα τις σχέσεις $R_1,\ldots,R_m$).

Ανακλαστικό+Μεταβατικό Κλείσιμο μιας διαδικής σχέσης R

- Η διαδική σχέση R είναι ένα σύνολο ($\subseteq A^2$)
- Η *ανακλαστική ιδιότητα* (ΑΙ) είναι ιδιότητα κλειστότητας (δείξτε το!)
- Η *μεταβατική ιδιότητα* (ΜΙ) είναι ιδιότητα κλειστότητας (το δείξαμε...)
- Το κλείσιμο, R*, της R ώς προς ΑΙ και ΜΙ λέγεται **Ανακλαστικό+Μεταβατικό Κλείσιμο της R**
- Εναλλακτικά:

R*={(a,b): υπάρχει *μονοπάτι* της R από το a στο b}

Ανακλαστικό+Μεταβατικό Κλείσιμο μιας διαδικής σχέσης R



Πολυπλοκότητα Αλγορίθμων

μια πρώτη ματιά

- Ζητούμενο:

  Πόσα βήματα χρειάζεται ένας αλγόριθμος για να ολοκληρωθεί;
- Ισοδύναμο ζητούμενο:

  Ποια συνάρτηση $f:N \to N$ αντιστοιχίζει το μέγεθος του προβλήματος, n, στον αριθμό των βημάτων, f(n), που απαιτούνται;
- Χρήσιμα εργαλεία: τάξη μεγέθους & ρυθμός αύξησης συναρτήσεων $f:N \to N$

Τάξη Μεγέθους – Ρυθμός Αύξησης

- **Τάξη μεγέθους** της f:N→N είναι το **σύνολο**:
  $O(f) = \{g/\ g:N\to N$ και $\exists$ σταθ. c,d: $g(n)\le cf(n)+d,\ \forall n\in N\}$
- $f\approx g$: $f\in O(g)$ και $g\in O(f)$
  - Η '≈' είναι σχέση ισοδυναμίας (δείξτε το)
- **Ρυθμός αύξησης**: κάθε κλάση ισοδυναμίας [f] που ορίζεται με βάση τη σχέση '≈'

Τάξη Μεγέθους – Ρυθμός Αύξησης
ενδιαφέροντα παραδείγματα (1)

1. $f(n)=31n^2+17n+3 \in O(n^2)$
   Απόδειξη: $31n^2+17n+3 \le 48\ n^2 + 3$
2. $n^2 \in O(f)$
   Απόδειξη: $n^2 \le 1f(n)+0$
3. Από (1) και (2) : $f(n) \approx n^2$
4. $f(n)=a_K n^K+\ldots+ a_1n+a_0 \in O(n^K)$ (με $c=\Sigma a_i$, $d=a_0$)
5. Αν $f(n)=a_K n^K+\ldots+ a_1n+a_0$ και
   $g(n)=b_L n^L+\ldots+ b_1n+b_0$ με $K>L>0$ τότε:
   - $f\notin O(g)$ αλλά $g \in O(f)$
   - $f \approx n^K$ και $g \approx n^L$

Τάξη Μεγέθους – Ρυθμός Αύξησης
ενδιαφέροντα παραδείγματα (2)

- Για όλα τα K: $n^K \in O(2^n)$ με $c=(2K)^K$ και $d=(K^2)^K$
- Απόδειξη:
  1. $n<2^n$ (αποδεικνύεται με επαγωγή)
  2. Για $n \leq K^2$: $n^K \leq (K^2)^K = d$

     Για $n \geq K^2$: $n^K \leq (2K)^K\, 2^n = c\, 2^n$

     Πράγματι: $n=\pi K+\upsilon \Rightarrow n< \pi K+K \Rightarrow n^K \leq K^K (\pi+1)^K \Rightarrow$
     $n^K < K^K (2^{\pi+1})^K = (2K)^K\, 2^{\pi K} \leq (2K)^K\, 2^n$
- Οι συναρτήσεις 5^n, n^n, $n!$, 2^{n^2} ακόμη μεγαλύτερο ρυθμό αύξησης

Αλγόριθμοι Ανακλαστικού/Μεταβατικού Κλεισίματος Διαδικής Συνάρτησης - Πολυπλοκότητα

- Αλγόριθμος #1 (ο προφανής):

  Υποθέτουμε ότι η σχέση $R \subseteq A^2$ όπου $A=\{a_1, a_2, \ldots, a_n\}$

  Αρχικοποίηση: $R^* = \varnothing$ και $n = |A|$

  FOR i =1,…,n DO

  FOR EACH $(b_1, b_2, \ldots, b_i) \in A^i$ DO

  IF $(b_1, b_2, \ldots, b_i)$ μονοπάτι στην R THEN πρόσθεσε το (b_1, b_i) στην R^*
- Πολυπλοκότητα (στη χειρότερη περίπτωση):
  - Για κάθε i ελέγχονται $\mathbf{|A^i| = n^i}$ i-αδες $(b_1, b_2, \ldots, b_i)$
  - Ο έλεγχος ‘αν είναι μονοπάτι’ μία i-άδα απαιτεί το πολύ **(i-1)<n** ελέγχους για το αν καθέ ζεύγος (b_j, b_{j+1}) με j=1,..,i-1 ανήκει στην R

  Άρα $f(n) \leq n\,(n + n^2 + \ldots + n^n) = n^2 + n^3 \ldots + n^{n+1} \Rightarrow \mathbf{f(n) \in O(n^{n+1})}$
- Καθόλου αποτελεσματικός (άκου $O(n^{n+1})$, το $O(n^{n+1})$ είναι χειρότερο κι από το $O(2^n)$!!!)

Αλγόριθμοι Ανακλαστικού/Μεταβατικού Κλεισίματος Διαδικής Συνάρτησης - Πολυπλοκότητα

- Αλγόριθμος #2 (λίγο καλύτερος):

  Υποθέτουμε ότι η σχέση $R \subseteq A^2$ όπου $A=\{a_1, a_2, \ldots, a_n\}$

  Αρχικοποίηση: $R^* = R \cup \{(\alpha_i, \alpha_i) / \alpha_i \in A\}$ και $n = |A|$

  WHILE υπάρχουν $\alpha_i, \alpha_j, \alpha_k \in A$ όπου $(\alpha_i, \alpha_j), (\alpha_j, \alpha_k) \in R$ αλλά $(\alpha_i, \alpha_k) \notin R^*$ DO

  πρόσθεσε το (α_i, α_k) στην R^*

- Πολυπλοκότητα (στη χειρότερη περίπτωση):
  - Ο έλεγχος 'υπάρχουν' στο εσωτερικό του WHILE απαιτεί το πολύ $3|\mathbf{A^3}|= \mathbf{3n^3}$ συγκρίσεις (για i,j,k=1…n). Το '3' αφορά τους 3 ελέγχους που απαιτούνται για τον εντοπισμό των διατεταγμένων ζευγών στις R και R*
  - Το WHILE θα εκτελεστεί το πολύ $|R^*| \leq |\mathbf{A^2}|= \mathbf{n^2}$ φορές γιατί σε κάθε εκτέλεση προστίθεται και ένα νέο διατεταγμένο ζεύγος στην R*.

  Άρα $f(n) \leq n^2 \times 3n^3 = 3n^5 \Rightarrow \mathbf{f(n) \in O(n^5)}$

- Πολύ καλύτερα! Πολυωνυμική πολυπλοκότητα!

Αλγόριθμοι Ανακλαστικού/Μεταβατικού Κλεισίματος Διαδικής Συνάρτησης - Πολυπλοκότητα

- Αλγόριθμος #3 (πολύ καλύτερος):

  Υποθέτουμε ότι η σχέση $R \subseteq A^2$ όπου $A=\{a_1, a_2, \ldots, a_n\}$

  Αρχικοποίηση: $R^* = R \cup \{(\alpha_i, \alpha_i) / \alpha_i \in A\}$ και $n = |A|$

```
FOR EACH j=1,2,…,n DO
    FOR EACH i=1,2,…,n DO
        FOR EACH k=1,2,…,n DO
            IF (αi, αj), (αj,αk) ∈ R* αλλά (αi,αk) ∉ R* THEN DO
                πρόσθεσε το (αi, αk) στην R*
```

- Πολυπλοκότητα (στη χειρότερη περίπτωση):
  - Λόγω των 3 nested FOR LOOPS έχουμε $\mathbf{n^3}$ επαναλήψεις.
  - Το IF κάθε επανάληψης απαιτεί 3 ελέγχους διατεταγμένων διάδων

  Άρα $f(n) \leq 3n^3 \Rightarrow \mathbf{f(n) \in O(n^3)}$

- Πολυωνυμική πολυπλοκότητα, καλύτερα από πριν.

Αλγόριθμοι Ανακλαστικού/Μεταβατικού Κλεισίματος Διαδικής Συνάρτησης – Απόδειξή;

- Οι τρείς προηγούμενοι αλγόριθμοι είναι **ορθοί** = παράγουν όντως την R*
- Αποδείξτε το...
- ... ή έστω επιδείξτε το (με ένα παράδειγμα)

Αλφάβητα και Γλώσσες

Οι **γλώσσες** είναι ένα εργαλείο 'τυπικής' αναπαράστασης (α) αλγορίθμων και (β) δομών δεδομένων που αυτοί επεξεργάζονται/παράγουν

Οι γλώσσες επεξεργάζονται συμβολοσειρές (strings) αποτελούμενες από σύμβολα που ανήκουν σε κάποιο **αλφάβητο**

Αλφάβητα – ορισμοί

- **Αλφάβητο (Σ)**: πεπερασμένο σύνολο συμβόλων
  - Το λατινικό αλφάβητο (πεζά) = {a,b,…,y,z}
  - Το διαδικό αλφάβητο = {1,0}
- **Συμβολοσειρά** (string) σε ένα *αλφάβητο Σ* : μια πεπερασμένου *μήκους* ακολουθία, w, συμβόλων του αλφαβήτου (aaabbb, butter, 1010111)
- $\Sigma^* = \{w/\ w$ συμβολοσειρά του $\Sigma\}$
  - Το Σ* περιλαμβάνει την κενή συμβολοσειρά **e**
- **Μήκος** συμβολοσειράς, |w| : |butter|=6, |e|=0
- Η συμβολοσειρά σαν συνάρτηση: $w:\{1,2,\ldots,|w|\}\rightarrow\Sigma$
  - Π.χ. για w=butter w(1)=b,w(2)=u, w(3)=t,w(4)=t,w(5)=e, w(6)=r

Αλφάβητα – πράξεις

- **Παράθεση** (concatenation)
  - Για $x, y \in \Sigma^*$: xoy (για συντομία xy) = 'πρώτα τα σύμβολα του x και μετά τα σύμβολα του y'
    - 0101 o 101 = 0101101
  - Μήκος: |xy|=|x|+|y|
  - Προσεταιριστική: (xy)z = x(yz) [οπότε γράφουμε xyz]
- **Υποσυμβολοσειρά (substring)** v μίας συμβολοσειράς w:
  - $\exists\ x, y \in \Sigma^*$: w=xvy
- **Κατάληξη (suffix)** v μίας συμβολοσειράς w:
  - $\exists\ x \in \Sigma^*$: w=xv
- **Πρόθεμα (prefix)** v μίας συμβολοσειράς w:
  - $\exists\ x \in \Sigma^*$: w=vx
- **'Δύναμη' w^i** :
  - $\mathbf{w^0} = e$ και $\mathbf{w^{i+1} = w^i\ o\ w}$

Αλφάβητα – πράξεις

- **Αντίστροφη** συμβολοσειρα w^R της w (τρείς ισοδύναμοι ορισμοί):
  1. w^R = 'η w γραμμένη από το τέλος προς την αρχή'
     – π.χ. $EGGS^R = SGGE$
  2. Αν w=e τότε w^R=w=e, αν |w|>0 τότε $w^R(i)=w(|w|-i+1)$
  3. Αν w=e τότε w^R=w=e, αν |w|=n+1>0 τότε $\exists a \in \Sigma$ και u $\in \Sigma^*$: w=ua και τότε $w^R = au^R$.
  – Ιδιότητα: $(xy)^R = y^R x^R$ (δείξτε το με επαγωγή)

Γλώσσες

- Γλώσσα L στο αλφάβητο Σ
  – L = {w / w ∈ Σ* και το w έχει κάποια ιδιότητα P}⊆ Σ*
    - Πεπερασμένες Γλώσσες = πεπερασμένα υποσύνολα του Σ*
    - Άπειρες Γλώσσες = απειροσύνολα υποσύνολα του Σ*
- Πρόταση: Αν το Σ είναι πεπερασμένο τότε το Σ* είναι αριθμήσιμο
  – Απόδειξη: Το Σ γράφεται $\Sigma=\{\alpha_1, \alpha_2, ..., \alpha_n\}$. Τότε τα στοιχεία του Σ* απαριθμούνται ως εξής: (1) Όλα τα n^k στοιχεία μήκους k απαριθμούνται πριν από αυτά με μήκος k+1. (2) Η απαρίθμιση γίνεται λεξικογραφικά ως προς τους δείκτες i=1,2, …, n των συμβόλων τους.
    - Π.χ. Σ={α,β}→ Σ*={e, α, β, αα, αβ, βα, ββ, ααα, ααβ, αβα, αββ, βαα, βαβ, ββα, βββ, αααα......}

Γλώσσες - Πράξεις

Οι Γλώσσες έχουν όλες τις πράξεις συνόλων και επιπλέον:

- **Παράθεση**: $L=L_1 o L_2$ (ή απλά $L=L_1L_2$)
  - $L=L_1 o L_2=\{w/w \in \Sigma^*$ και $\exists x \in L_1, y \in L_2$ ώστε $w=xoy\}$
- **Kleene star**: L^*
  - $L^* = \{w/\ w \in \Sigma^*: w=w_1 o w_2 o \ldots o w_k$ για $k \geq 0$ και $w_1,w_2,\ldots,w_k \in L\}$='όλες οι συμβολοσειρές που προκύπτουν από παραθέσεις συμβολοσειρών της L (περιλαμβανομένης και της κενής)'
- $L+ = L o L^*$ (είναι το κλείσιμο της L ως προς την συνάρτηση *παράθεση*)

Πεπερασμένη Αναπαράσταση Γλωσσών

- Οι πεπερασμένες γλώσσες έχουν έτσι κι αλλοιώς πεπερασμένη αναπαράσταση
- Οι άπειρες γλώσσες έχουν;
  - **ΝΑΙ υπό προϋποθέσεις**
  - ΔΕΝ μπορούν όλες οι γλώσσες (ενός αλφαβήτου Σ) να αναπαρασταθούν (περιγραφούν) από πεπερασμένο αριθμό συμβόλων κάποιου αλφαβήτου Σ_L, γιατί:
    - Το σύνολο, Σ_L^*, των δυνατών περιγραφών πεπερασμένου μήκους είναι **μετρήσιμο**, ενώ
    - Το σύνολο των δυνατών γλωσσών, 2^{Σ^*}, είναι **μη μετρήσιμο**!

Πεπερασμένη Αναπαράσταση Γλωσσών-Κανονικές Γλώσσες

Κανονικές Εκφράσεις (ΚΕ) σε αλφάβητο Σ: το σύνολο των συμβολοσειρών του $\Sigma_L = \Sigma \cup \{(,\ ),\ \varnothing,\ \cup,\ *\}$ που παράγονται σύμφωνα με τα παρακάτω:

1. Το ∅ και κάθε στοιχείο του Σ είναι ΚΕ
2. Αν οι συμβολοσειρές α και β είναι ΚΕ τότε και το (αβ) είναι ΚΕ
3. Αν οι συμβολοσειρές α και β είναι ΚΕ τότε και το (α ∪ β) είναι ΚΕ
4. Αν η συμβολοσειρά α είναι ΚΕ τότε α* είναι ΚΕ
5. Οποιαδήποτε συμβολοσειρά ΔΕΝ προκύπτει από τα 1 ώς 4 ΔΕΝ είναι ΚΕ

Πεπερασμένη Αναπαράσταση Γλωσσών-Κανονικές Γλώσσες

- Κάθε κανονική έκφραση α περιγράφει μία **κανονική γλώσσα** $L(\alpha) \subseteq \Sigma^*$ εάν θεωρήσουμε ότι:
  - Το σύμβολο ∪ σημαίνει ένωση γλωσσών
  - Το σύμβολο * σημαίνει το Kleene star μίας γλώσσας
  - Η τοποθέτηση πλάι-πλάι σημαίνει παράθεση γλωσσών
  - Οι παρενθέσεις (και) όρίζουν προτεραιότητα
- Αναλυτικότερα η γλώσσα $L(\alpha)$ παράγεται αναδρομικά ώς εξής:
  - $L(\varnothing) = \varnothing$ (κενή γλώσσα) και $L(a) = \{a\}$ για $\forall a \in \Sigma$
  - Αν α,β ΚΕ τότε $L(\ (\alpha\beta)\ ) = L(\alpha)L(\beta)$ (παράθεση γλωσσών)
  - Αν α,β ΚΕ τότε $L(\ (\alpha\cup\beta)\ ) = L(\alpha) \cup L(\beta)$ (παράθεση γλωσσών)
  - Αν α ΚΕ τότε $L(\alpha^*) = L(\alpha)^*$ (Kleene star γλώσσας)

Πεπερασμένη Αναπαράσταση Γλωσσών-Κανονικές Γλώσσες – Παραδείγματα:

#1: Έστω $\Sigma=\{0,1\}$ και ΚΕ $\alpha = 0^*10^*010^*(10^*\cup\varnothing^*)$ τότε:

$L(\alpha) = L(0^*) \circ L(1) \circ L(0^*) \circ L(0) \circ L(1) \circ L(0^*) \circ L(10^* \cup\varnothing^*)$

$= L(0^*)\circ L(1) \circ L(0^*) \circ L(0) \circ L(1) \circ L(0^*) \circ \big(L(1) \circ L(0^*) \cup L(\varnothing^*)\big)$

= οι συμβολοσειρές που έχουν 2 ή 3 εμφανίσεις του συμβόλου 1 εκ των οποίων η πρώτη και η δεύτερη **δεν είναι συνεχόμενες**, π.χ.

000100100, 101100000, αλλά όχι 000**11**000100

Πεπερασμένη Αναπαράσταση Γλωσσών-Κανονικές Γλώσσες – Παραδείγματα:

#2: Σ={**a**,**b**} και ΚΕ α = **((a∪b)*a)**, τότε:

L(α) =

L(**(a∪b)*a**)L(**a**) =

L(**(a∪b)***)**{a}** =

(L(**a**) ∪L(**b**))***{a}** =

{{**a**} ∪{**b**}}*{**a**} =

{**a**,**b**}*{**a**} =

{w/w∈ {**a**,**b**}* και w τελειώνει με **a**} =

{οποιαδήποτε παράθεση των **a** και **b** που τελειώνει με **a**}