1ο μέρος

Models of Computation

Πρότυπα Υπολογισμού

Βασικά Πρότυπα Υπολογιστών και Υπολογισμών

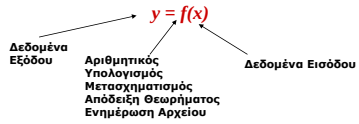
Αλγόριθμος = Μηχανιστική Διαδικασία

που εκτελεί μια

Μηχανή = Υπολογιστής

Έτσι εκτελείται ένας

Υπολογισμός



Βασικά Πρότυπα Υπολογιστών και Υπολογισμών

Η f αναλύεται σε μια ακολουθία

$$f = f_1, f_2, \ldots, f_n$$

$$\left.\begin{array}{l} y_1 = f_1(x) \\ y_2 = f_2(y_1) \\ \cdot \\ \cdot \\ y_{n-1} = f_{n-1}(y_{n-2}) \\ y_n = f_n(y_{n-1}) \end{array}\right\} \Pi\rho\acute{o}\gamma\rho\alpha\mu\mu\alpha$$

Είδη Μηχανών - 1

Βασική Μηχανή (ΒΜ)

(Ι, Ο, λ)

Ι = σύνολο εισόδων

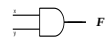
Ο = σύνολο εξόδων

λ = Συνάρτηση εξόδου λ : Ι → Ο

Ι , Ο πεπερασμένα

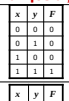
π.χ. Λογική πύλη AND

Λογική πύλη AND

όνομα	Συμβολισμός	Συνάρτηση	Πίνακας αληθείας
AND		$F = xy$	

- Η έξοδος της πύλης μια δεδομένη χρονική στιγμή εξαρτάται από τις τιμές των εισόδων την ίδια χρονική στιγμή.
- Την ιδιότητα αυτή έχουν όλα τα λεγόμενα συνδυαστικά κυκλώματα (δηλ. αυτά είναι βασικές μηχανές)
- Θα δούμε αργότερα και άλλες λογικές πύλες και συνδυαστικά κυκλώματα

Λογικές πύλες

όνομα	Συμβολισμός	Συνάρτηση	Πίνακας αληθείας
AND		$F = xy$	
OR		$F = x+y$	
NOT		$F = \overline{x}$	

Είδη Μηχανών - 2

Μηχανή Πεπερασμένων Καταστάσεων (FSM)

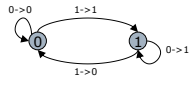
(S, I, O, δ, λ)

- I = σύνολο εισόδων
  O = σύνολο εξόδων
  S = σύνολο καταστάσεων
  Συνάρτηση εξόδου λ: IxS → O κατά Mealy
  Συνάρτηση καταστάσεων δ : IxS → S
  I,O,S πεπερασμένα
- Η έξοδος της μηχανής είναι ουσιαστικά συνάρτηση της παρούσας εισόδου αλλά και όλων των παρελθόντων εισόδων (που χωρίζονται σε πεπερασμένο αριθμό κλάσεων, δηλ., στις διάφορες καταστάσεις της μηχανής)
- π.χ. Διακόπτης On-Off (Push-Button)

Παραδείγματα

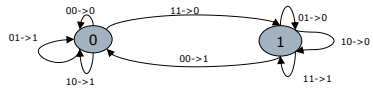
Διακόπτης ON/OFF

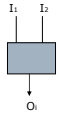
S \ I	0	1
0	0/0	1/1
1	1/1	0/0



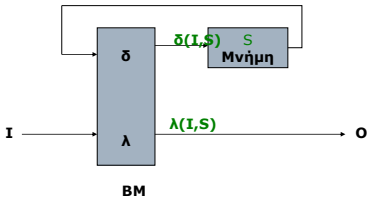
Σειριακός Αθροιστής

S \ $I_1 I_2$	00	01	10	11
0	0/0	0/1	0/1	1/0
1	0/1	1/0	1/0	1/1





Δομή ακολουθιακού κυκλώματος



ΒΜ

Ορισμός ακολουθιακού κυκλώματος

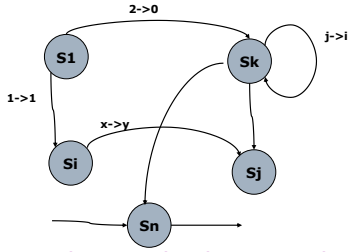
M = (S, I, O, δ, λ)

Πίνακας καταστάσεων

S\I	1	2	...	j	...	m
S_1	S_{11}/O_{11}	S_{12}/O_{12}	..	S_{1j}/O_{1j}	..	S_{1m}/O_{1m}
S_2	S_{21}/O_{21}	S_{22}/O_{22}	..	S_{2j}/O_{2j}	..	S_{2m}/O_{2m}
...	..	..	..	..	..	..
S_i	S_{i1}/O_{i1}	S_{i2}/O_{i2}	..	S_{ij}/O_{ij}	..	S_{im}/O_{im}
...	..	..	..	..	..	..
S_n	S_{n1}/O_{n1}	S_{n2}/O_{n2}	..	S_{nj}/O_{nj}	..	S_{nm}/O_{nm}

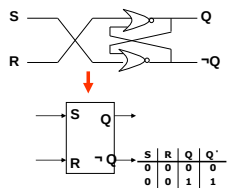
Γενικό ακολουθιακό κύκλωμα

Διάγραμμα Καταστάσεων



*** Που φυλάσσεται η κατάστασή; Σε μνημονικά στοιχεία

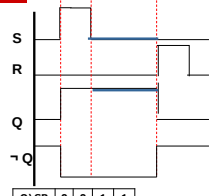
Δικατάστατο Μνημονικό στοιχείο: Set – Reset flip-flop - 1 bit



S	R	Q	Q΄
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	-
1	1	1	-

Πίνακες αλήθειας

Επόμενη κατάσταση
Q΄= S+ ¬ RQ με SR = 0



Q\SR	0 0	0 1	1 1	1 0
0	0	0	-	1
1	1	0	-	1

Άσκηση 1η : Μπουτόν 3-5

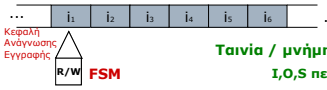
- Ημερομηνία ανάρτησης:
- Ημερομηνία-Προθεσμία υποβολής μέσω Moodle: 1
- Filename: forename.surname _Bouton3-5, filetype doc OR pdf

επί ποινή μηδενισμού

- (α) Να σχεδιάσετε δύο μηχανές πεπερασμένων καταστάσεων που κάθε μια να ανάβει και να σβήνει ένα φώς αντίστοιχα σε πολλαπλάσια του 3, και αντίστοιχα του 5, πατήματα ενός μπουτόν (αρχικά το φως σβηστό, μηδέν πάτημα).
- Να δώσετε τους σχετικούς πίνακες και διαγράμματα καταστάσεων τους
- (β) Να συνδυάσετε αυτές τις δύο μηχανές πεπερασμένων καταστάσεων με αυτή που ανάβει και σβήνει ένα φως σε πολλαπλάσια του 2 πατήματα ενός μπουτόν ώστε να προκύψει μια μηχανή που ανάβει και σβήνει το φως σε πολλαπλάσια του 3 και του 5 πατήματα του μπουτόν. Δώστε το σχετικό σχηματικό διάγραμμα διασύνδεσης των τριών μηχανών και ότι άλλο βοηθητικό εξάρτημα νομίζετε ότι θα χρειαστεί στην διασύνδεσή τους.

Είδη Μηχανών -3

Μηχανή Turing (S, I, β, t_0, s_0, H) Alan Turing 1936

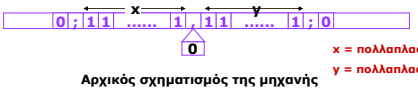


Συνάρτηση επομένου βήματος β=<δ, λ, κ>
- Συνάρτηση εξόδου λ: IxS → O
- Συνάρτηση καταστάσεων δ: IxS→ S
- Συνάρτηση κίνησης κ: S → {L,R,N}

t_0 = αρχική θέση R/W κεφαλής
s_0 = αρχική κατάσταση μηχανής
H = κατάσταση τερματισμού (Holt)

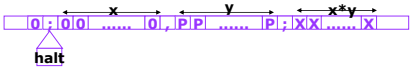
Π.χ. Πολλαπλασιασμός

Πολλαπλασιασμός με μηχανή Turing



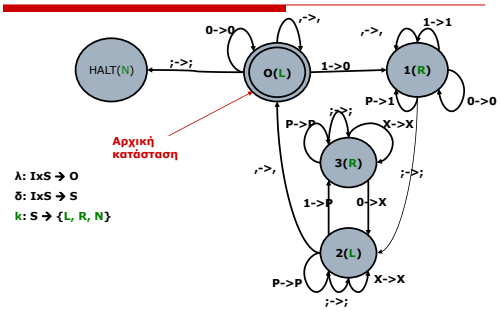
x = πολλαπλασιαστής
y = πολλαπλασιαστέος

Αρχικός σχηματισμός της μηχανής



Τελικός σχηματισμός της μηχανής

Πολλαπλασιασμός με μηχανή Turing



Άσκηση 2η : Turing διαίρεσης

- Ημερομηνία ανάρτησης:
- Ημερομηνία-Προθεσμία υποβολής:
- Filename: forename.surname _Bouton3-5, filetype doc OR pdf

επί ποινή μηδενισμού

- Να σχεδιαστεί μηχανή Turing που να κάνει την ακέραιη διαίρεση δύο φυσικών αριθμών που δίνονται σε μοναδιαία μορφή. Τα αποτελέσματα πρέπει να είναι το ακέραιο πηλίκο και το υπόλοιπο.
- Να ληφθεί υπόψη και η περίπτωση που ο διαιρέτης να είναι μηδέν.
- (α) Να δώσετε τη μορφή της αρχικής κατάστασης της ταινίας και την τελική της στις δυο περιπτώσεις (διαιρέτης μηδέν ή όχι).
- (β) Να δώσετε το διάγραμμα λειτουργίας της μηχανής Touring και να το συνδεύετε με κείμενο επεξήγησης

Ισχύς της μηχανής Turing

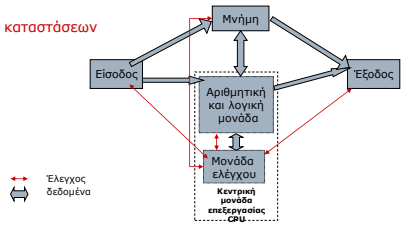
- Θέση του Church
  - Κάθε υπολογισμός για τον οποίο υπάρχει αποτελεσματική διαδικασία μπορεί να πραγματοποιηθεί με μία μηχανή Turing.
- Θέση του Turing
  - Αποτελεσματική διαδικασία είναι αυτή που μπορεί να διεκπεραιωθεί από μία μηχανή Turing.

Καθολική μηχανή Turing (UTM)

- Προσομοιώνει οποιαδήποτε άλλη μηχανή Turing.
- Η ταινία περιέχει και την περιγραφή της υπό προσομοίωση μηχανής Turing.
- Μία UTM χρειάζεται
  - t το πλήθος των συμβόλων εισόδου
  - S το πλήθος των καταστάσεων
  - Αρκεί t*S < 30

Υπολογιστής ≈ UTM

- Σύγκριση
  - Μνήμη
  - Αριθμός καταστάσεων

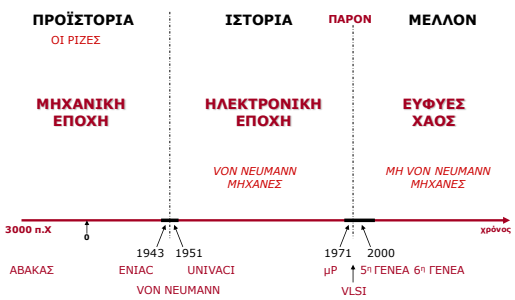


Αρχιτεκτονική von Neumann

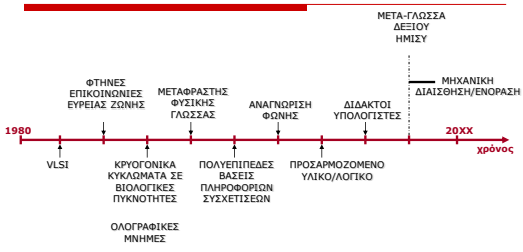
- Τυπικό διάγραμμα υπολογιστή
- Χαρακτηριστικά:
  - **Στενωπός – μποτιλιάρισμα (bottleneck)**
    - **Μνήμη ↔ K.M.E – μηχανή**
    - **Εντολή αντικατάστασης – γλώσσες**
  - **Ροή προγράμματος**
    - **Καθορίζεται από τις εντολές-διαταγές**
    - **Απαριθμητής εντολών**

Η ιεραρχία Υλικού - Λογισμικού

Η ΕΞΕΛΙΞΗ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (1/2)



Η ΕΞΕΛΙΞΗ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ (2/2)



ΕΞΕΛΙΞΗ ΠΡΟΣ ΤΗΝ ΠΕΡΙΟΧΗ ΤΟΥ ΔΕΞΙΟΥ ΗΜΙΣΥ ΤΟΥ ΕΓΚΕΦΑΛΟΥ

Παράδειγμα επίλυσης προβλήματος (με αυξανόμενη απόδοση) 1/4

Πρόβλημα 1: **Να υπολογιστεί το άθροισμα**
Σ=1 +2+3+…+1000

- **1η Λύση: Σειριακά (1 άνθρωπος)**
  αθροίζοντας 2 αριθμούς κάθε φορά
  1+2=3
  3+3=6
  6+4=10
  ……
  ……

Απαιτούνται 999 βήματα

Παράδειγμα επίλυσης προβλήματος (με αυξανόμενη απόδοση) 2/4

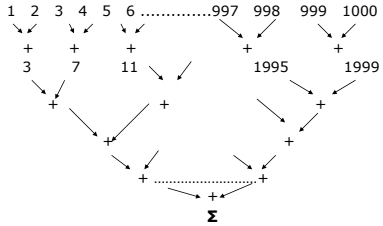
- **2η Λύση: Σωληνοειδώς (2 άνθρωποι)**

1ος άνθρωπος	2ος άνθρωπος
1+2=3	3+4=7
5+6=11	7+3=10
7+8=15	10+11=21
9+10=19	21+15=36
11+12=23	36+19=55
…	55+23=78
995+996=1991	….
997+998=1995	494515+1991=496506
999+1000=1999	496506+1995=498501
	498501+1999=500500

Απαιτούνται 500 βήματα
Πόσα βήματα για 3, 4,… Ανθρώπους;

Παράδειγμα επίλυσης προβλήματος (με αυξανόμενη απόδοση) 3/4

- **3η Λύση: Παράλληλα (500 άνθρωποι)**



Απαιτούνται $\lfloor \log_2 1000 \rfloor = 10$ βήματα

Παράδειγμα επίλυσης προβλήματος (με αυξανόμενη απόδοση) 4/4

- **4η Λύση: Με ευφυΐα**

Αναγνωρίζεις ότι το ζητούμενο είναι άθροισμα αριθμητικής προόδου και εφαρμόζεις τον τύπο του αθροίσματος

Σ=1+2+3+…+1000=(1+1000)1000/2

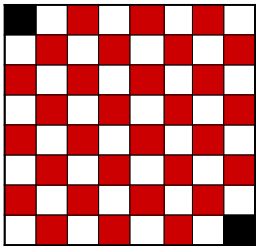
Απαιτούνται 3 βήματα!

Παράδειγμα επίλυσης προβλήματος (με ευφυΐα)

- Πρόβλημα 2:

Μπορεί να πλακοστρωθεί η αυλή με πλακίδια του δεδομένου τύπου;

Απάντηση: ΟΧΙ



ΕΓΚΕΦΑΛΟΣ

Γλωσσικά προϊόντα

- Υπολογισμοί:
  - $y = x^2$
  - $y = \sqrt{25 - 1.3*5}$
- Συσχετίσεις:
  - Γεωργική παραγωγή – βροχόπτωση
  - ΑΕΠ - Γεννητικότητα

Μη Γλωσσικά προϊόντα

- **Συνειρμοί:**
  - Όχι, δεν θέλω!
  - Μαύρη γάτα -> θα τρακάρω
- **Συμπερασμοί:**
  - 3,5, ?, 11, 13, 17, ...
  - Σε γνωρίζω από τη ----
    του σπαθιού --- τρομε--
    Σε ------- από την όψη
    που με βία ----- τη γη
- **Παρεκτάσεις:**
  - Διαμόρφωση μιας θεωρίας
  - Ζωγραφικός πίνακας, Μελωδία, κλπ

Σύγκριση ανθρώπινου εγκεφάλου και ηλεκτρονικού υπολογιστή

- Εγκέφαλος
  - ≈ 40 δις νευρώνες
  - 1000 – 10000 διασυνδέσεις I/O ανά νευρώνα
  - 100 τρις συνδέσεις
  - Ταχύτητα παλμού 16 km/h
- Υπολογιστής
  - 1 MBytes –1TMBytes μνήμη RAM και έως κάποια TBytes σκληρός δίσκος.
  - 4 I/O ανά πύλη
  - Αραιά διασύνδεση
  - Σήματα: ταχύτητα φωτός 300000 km/s

Όρια Υπολογισμού

- **Όριο Bremermann** (1962)
  - **Ζωντανός ή τεχνητός υπολογιστής μπορεί να επεξεργαστεί $2x10^{47}$ bits/gr.sec .**
  - **Υπολογιστής με μέγεθος ίσο με τη Γη:**

$$6*10^{27}\,gr \times 10^{10}\,\text{χρόνια} \Rightarrow 10^{93}\,\text{bits}$$

Δυνατές καταστάσεις μνήμης 10^6 θέσεων = 10^{300000}

Δυνατές κινήσεις στο σκάκι = 10^{120}

Limits of Computations -2

- Ας υποθέσουμε ότι το όριο είναι αληθές, Τώρα
  - Υποθέστε ότι προστατεύουμε έναν υπολογιστή με ένα κωδικό των 40 δεκαδικών ψηφίων.
  - Σπάσιμο αυτού του κωδικού στη χειρότερη περίπτωση απαιτεί να δοκιμάσουμε 10^{40} συνδιασμούς.
  - Ένας υπολογιστή που εργάζεται με ταχύτητα το όριο Bremermann, θα απαιτήσει λιγότερο από ένα second, ακόμη και εάν ζυγίζει μόνο 1 gram.

Limits of Computations -3

Για κωδικό των 100 δεκαδικών ψηφίων ;

- Εάν προστατευόμεθα με 100 ψηφία, θα είμαστε ασφαλείς, ακόμη και εάν είχαμε ένα υπολογιστή 10 τόνων, για τουλάχιστον

  $10^{100} * \log_2(10) / (10^7 * 2 * 10^{47})$seconds.

- Δηλαδή, αιώνια.

Η εκθετική πολυπλοκότητα είναι καλή για κωδικούς ασφαλείας!

Limits of Computations -4

Ένας Υπολογιστής στο μέγεθος της γης μπορεί να κάνει περίπου10^{75} πράξεις το δευτερόλεπτο υποθέτοντας ότι κάθε κλειδί μπορεί να δοκιμαστεί με μια μόνο πράξη. Τότε

Κλειδί κρυπτογράφησης με μήκος

1. 128 bits σπάει σε 10^{-36} δευτερόλεπτα
2. 256 bits σπάει σε 2 λεπτά
3. 512 bits σπάει σε 10^{72} χρόνια