Θεμελιώδη Θέματα Επιστήμης Υπολογιστών

1η Σειρά Ασκήσεων

Χρήστος Τσούφης
ΣΗΜΜΥ

Άσκηση 1

hint: · $ab \bmod n = (a \bmod n)(b \bmod n) \bmod n$

· κριτήριο διαιρετότητας αριθμού με το 9.

$$2^{29} \bmod 9 = (2^{14} \bmod 9)(2^{15} \bmod 9) \bmod 9$$

$$= \Big((2^7 \bmod 9)(2^7 \bmod 9) \bmod 9 \cdot (2^8 \bmod 9)(2^7 \bmod 9) \bmod 9\Big) \bmod 9$$

$$= \Big(((2 \cdot 2) \bmod 9) \cdot ((4 \cdot 2) \bmod 9)\Big) \bmod 9$$

$$= 32 \bmod 9 = 5 \quad (*)$$

Άρα ο αριθμός 2^{29} εάν διαιρεθεί με το το 9 αφήνει υπόλοιπο 5.

Έχουμε $2^{29} = 2^{27} \cdot 2^2 = (2^3)^9 \cdot 4 = 4 \cdot 8^9 \Rightarrow 2^{29} = 4 \cdot 8^9$

Ψάχνουμε το ψηφίο που λείπει από τον 2^{29}. Έστω το ψηφίο x.

Το άθροισμα όλων των ψηφίων θα είναι $0+1+2+3+\ldots+9 = 45$

Άρα, το άθροισμα όλων των ψηφίων εκτός του x θα είναι $45-x$.

Για τον αριθμό A με A_i τα αντίστοιχα ψηφία ισχύει:

$A \bmod 9 = (A_0 + A_1 + \ldots + A_n) \bmod 9$ (από διαφάνειες)

Συνεπώς, $2^{29} \bmod 9 = (45 - x) \bmod 9 \Rightarrow$

$$\overset{(*)}{\Rightarrow} 5 = 45 \cancel{\bmod} 9 + (-x) \bmod 9$$

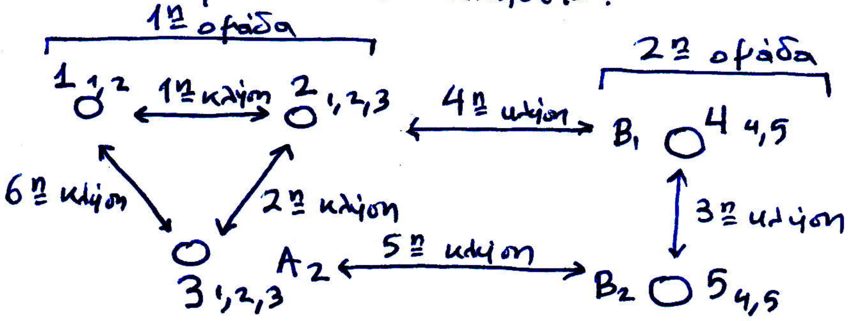
$$\Rightarrow 5 = (-x) \bmod 9$$

$$\Rightarrow x = -4$$

Άρα το ψηφίο που λείπει είναι το 4.

Άσκηση 2

Χωρίζουμε τους 5 φίλους σε δύο ομάδες. Μία των 3 ατόμων και μία των 2 ατόμων.
Οι δείκτες στο ακόλουθο σχήμα δείχνουν τις πληροφορίες που γνωρίζουν οι φίλοι μετά τις κλήσεις.



$1 \xleftrightarrow{\text{καλεί}} 2$, $2 \xleftrightarrow{\text{καλεί}} 3$, άρα οι 2,3 έχουν επίγνωση όλων των μυστικών της ομάδος τους

$4 \xleftrightarrow{\text{καλεί}} 5$, άρα οι 4,5 -11-

Έστω $2 = A_1$, $3 = A_2$, $4 = B_1$, $5 = B_2$

Καλούν $A_1 \longleftrightarrow B_1$

$A_2 \longleftrightarrow B_2$ άρα οι 2,3,4,5 γνωρίζουν όλα τα μυστικά

Απομένει 1 ακόμα κλήση του 1 με οποιονδήποτε από τους υπόλοιπους, ώστε να γνωρίζουν όλοι όλα τα μυστικά.
Συνολικά 6 κλήσεις για 5 άτομα ($N=5$, άρα $2N-4 = 6$ κλήσεις)

Γενικά

- Για $N=1$: 0 κλήσεις
- Για $N=2$: 1 κλήση ($1 = 2\cdot 2 - 3 = 2N-3$)
- Για $N=3$: 3 κλήσεις (1 καλεί 2, 2 καλεί 3, 3 καλεί 1)
  (που είναι πάλι $3 = 2\cdot 3 - 3 = 2N-3$)

Άρα για $N=2$ και $N=3$ απαιτούνται $2N-3$ κλήσεις

• Για $N \geq 4$ αποδεικνύεται ότι:

- Χωρίζουμε τους N σε δύο ομάδες, όπου αν N περιττό, η μία ομάδα έχει ένα φίλο περισσότερο.
- Στην πρώτη ομάδα (A), ο φίλος 1A καλεί 2A, 2A καλεί 3A, …, προτελευταίος ομάδος A καλεί τελευταίο ομάδος A.
- Στην δεύτερη ομάδα (B), ο φίλος 1B καλεί 2B, 2B καλεί 3B, …, προτελευταίος ομάδος B καλεί τελευταίο ομάδος B
- Μετά από $N-2$ κλήσεις, σε κάθε ομάδα δύο φίλοι θα γνωρίζουν όλα τα μυστικά της ομάδος τους.

Έστω X_1, X_2 οι δύο αυτοί φίλοι της πρώτης και Y_1, Y_2 της δεύτερης.
(στο παραδ. με τους 5 φίλους είχαμε τους A_1, A_2 και B_1, B_2 αντίστοιχα)
Τώρα, καλεί ο $X_1 \leftrightarrow Y_1$ και ο $X_2 \leftrightarrow Y_2$. Οπότε οι 4 αυτοί φίλοι γνωρίζουν όλα τα μυστικά. Για τους υπόλοιπους $N-4$ φίλους χρειάζονται ακριβώς $N-4$ κλήσεις. Άρα, συνολικά:

$$(N-2)+2+(N-4) = 2N-4 \text{ κλήσεις.}$$

Συνεπώς, οι ελάχιστες κλήσεις είναι ακριβώς:

- 0, για $N=1$
- $2N-3$, για $N=2,3$
- $2N-4$, για $N \geq 4$

• Απόδειξη ότι για $N \geq 4$ οι ελάχιστες κλήσεις είναι $2N-4$:

Έστω ότι για $N \geq 4$ η πλήρης ανταλλαγή μυστικών μπορεί να γίνει με λιγότερες από $2N-4$ κλήσεις. Έστω π.χ. ότι μπορεί να γίνει με $2N-5$ κλήσεις. Όμως, αυτό σημαίνει ότι για $N=4$ οι $2\cdot 4-5=3$ κλήσεις θα επαρκούν για πλήρη ανταλλαγή μυστικών, πράγμα που φυσικά δεν ισχύει αν εξεταστούν 3 κλήσεις μεταξύ 4 ατόμων.
Συνεπώς, για την περίπτωση του $N=4$ καταλήγει σε άτοπο, δηλαδή ο ελάχιστος αριθμός για $N=4$ είναι $2N-4=4$ κλήσεις

Τώρα, θα εξεταστεί η περίπτωση για $N>4$.

Γνωρίζουμε ότι η προσθήκη ενός ακόμα φίλου σε ένα δίκτυο N-φίλων έχει ως συνέπεια την αύξηση του αριθμού των κλήσεων κατά 2. Αυτό συμβαίνει διότι, ο $(N+1)$στος φίλος που προστέθηκε θέλει μια κλήση, ώστε να πει αρχικά το μυστικό του στον επόμενο και άλλη μια κλήση, ώστε όταν οι X_1, Y_1, X_2, Y_2 (οι 4 φίλοι που γνωρίζουν όλα τα μυστικά όπως περιγράψαμε <u>γενικά</u> ότι αρκούν $2N-4$ κλήσεις) γνωρίσουν όλα τα μυστικά, να πει ένας από αυτούς όλα τα μυστικά στον $(N+1)$στο φίλο που προστέθηκε. Άλλωστε, για $N+1$ έχουμε $2(N+1)-4 =$
$= \underline{2N-4} + \underline{\underline{2}}$ κλήσεις

- Δείξαμε ότι για $N=4$ απαιτούνται $2N-4=4$ κλήσεις τουλάχιστον.
- για $N=4+1=5$ σύμφωνα με το παραπάνω συμπέρασμα απαιτούνται τουλάχιστον $4+\underline{2}=6$ κλήσεις με $6=2N-4$, για $N=5$
  Αντίθετα, δεν αρκούν $2N-5=5$ κλήσεις
- για $N=5+1=6$ απαιτούνται τουλάχιστον $6+\underline{2}=8$ κλήσεις (όσες για $N=5$ + τις επιπλέον 2 με την προσθήκη του έκτου φίλου) όπου $8=2N-4$, για $N=6$
  Αντίθετα, δεν αρκούν $2N-5=7$ κλήσεις

κλπ για έξτρα φίλους.

Επομένως, τόσο για $N=4$ όσο και για $N>4$, οι $2N-5$ κλήσεις δεν επαρκούν και καταλήγουμε σε άτοπο. Έχοντας δείξει ότι οι $2N-4$ κλήσεις επαρκούν, συμπεραίνουμε ότι οι $2N-4$ κλήσεις είναι οι ελάχιστες δυνατές για $N \geq 4$.

▷ Με πιο αυστηρό μαθηματικό τρόπο:

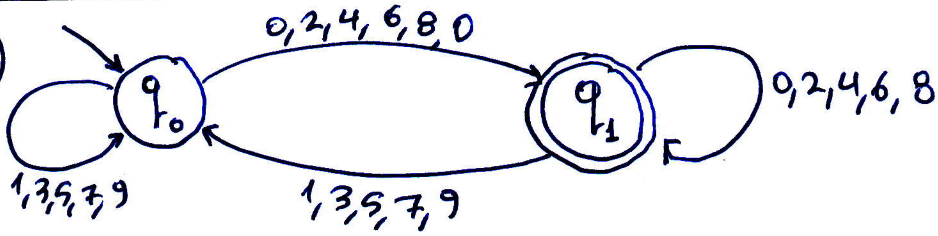
Έστω $n+1$ φίλοι. Ο $n+1$ καλεί ένα τυχαίο φίλο j ο οποίος σε $\varphi(n)$ κλήσεις θα έχει μεταδώσει την πληροφορία. Έπειτα ο $n+1$ καλεί τον j για να μάθει τα μυστικά των υπολοίπων. Άρα: $\varphi(n+1)-\varphi(n) \geq 2 \Rightarrow$

$$\Rightarrow \sum_{m=5}^{n+1} [\varphi(m+1)-\varphi(m)] \geq \sum_{m=5}^{n+1} 2 \Rightarrow \varphi(n+2) - \cancel{\varphi(5)}^{6} \geq 2(n+2-5)$$

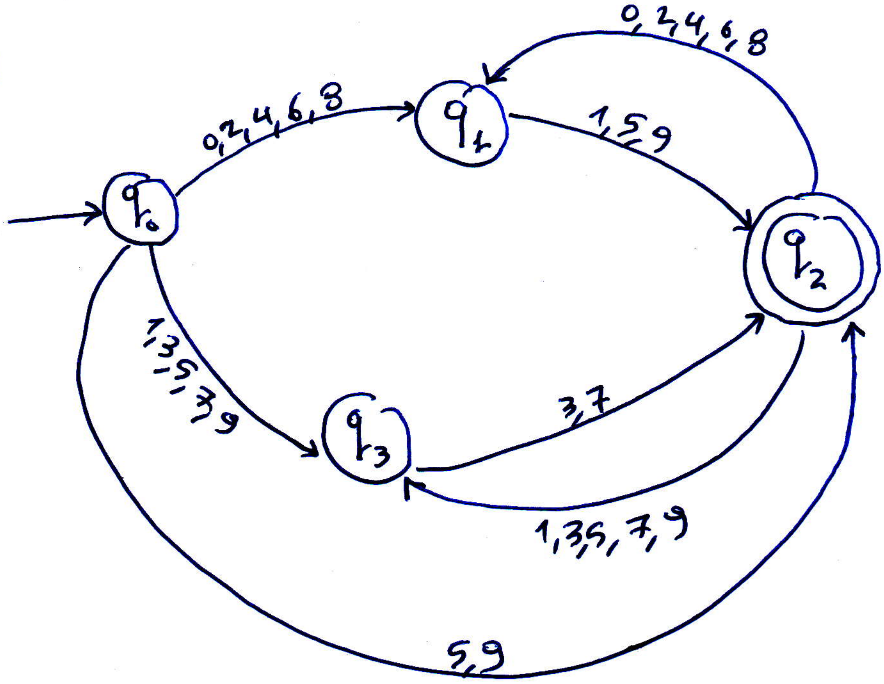
$$\Rightarrow \varphi(n+2) \geq 2n-6+6 = 2n \overset{n'=n+2}{\Longrightarrow} \varphi(n') \geq 2(n'-2) \Rightarrow \varphi(n) \geq 2n-4$$

Άσκηση 3

i)

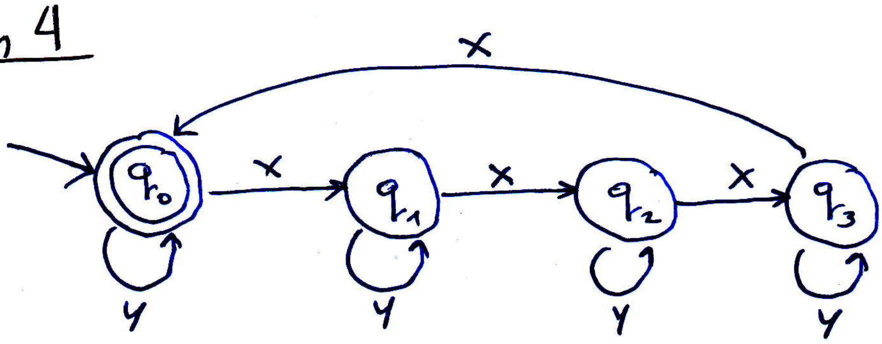


ii)

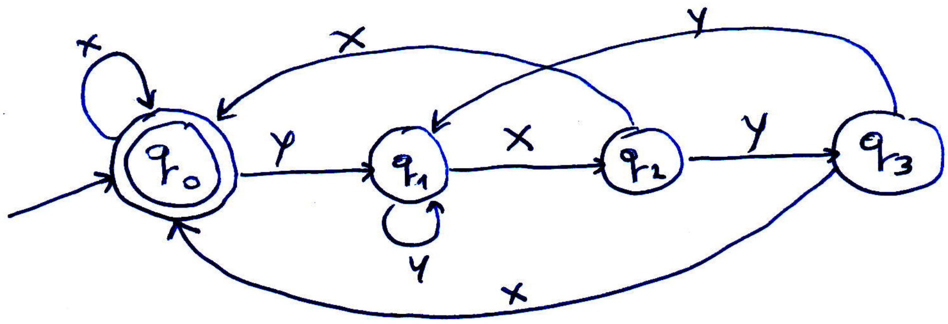


Άσκηση 4

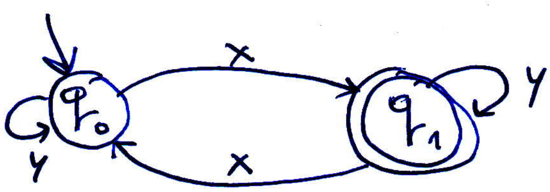
a)



β)

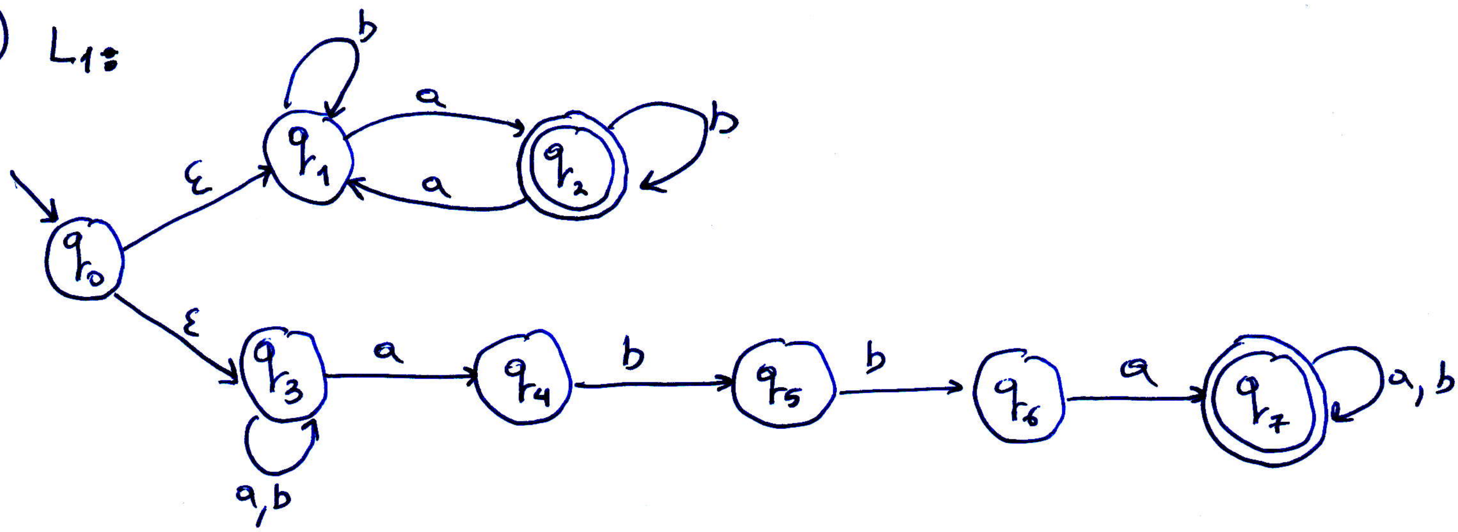


γ)

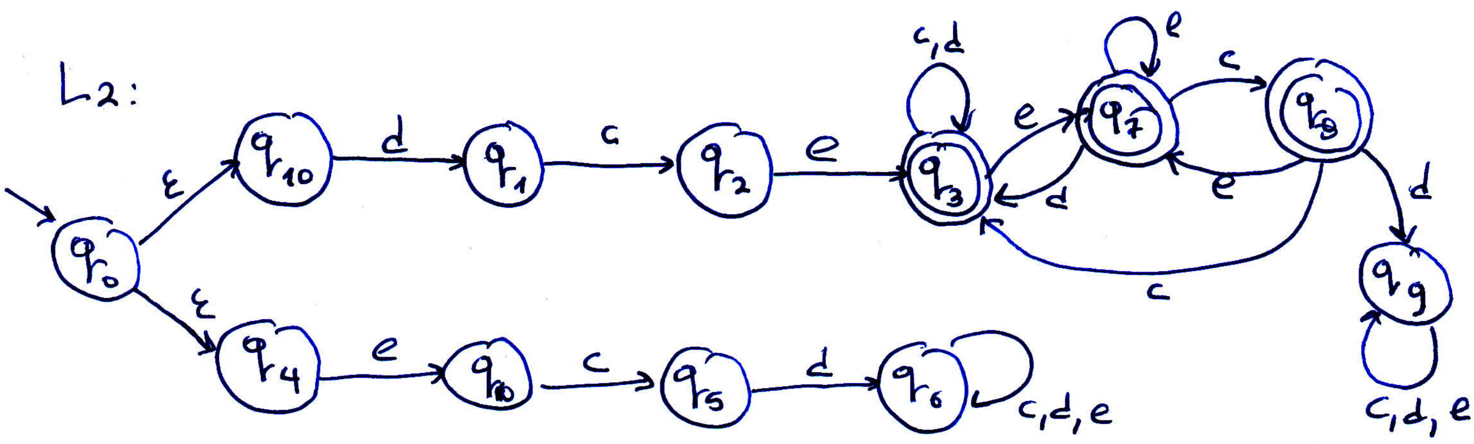


Άσκηση 5

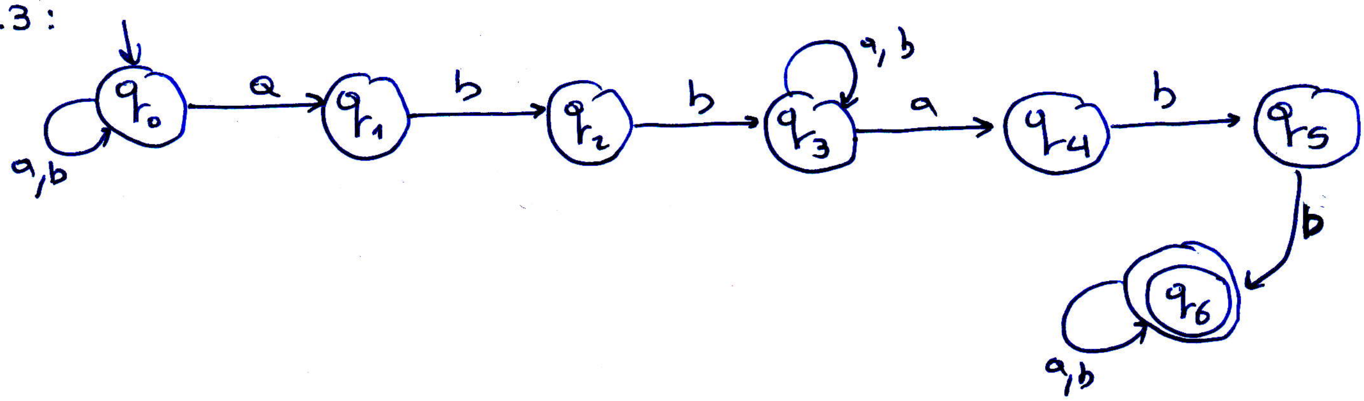
i) L_1:



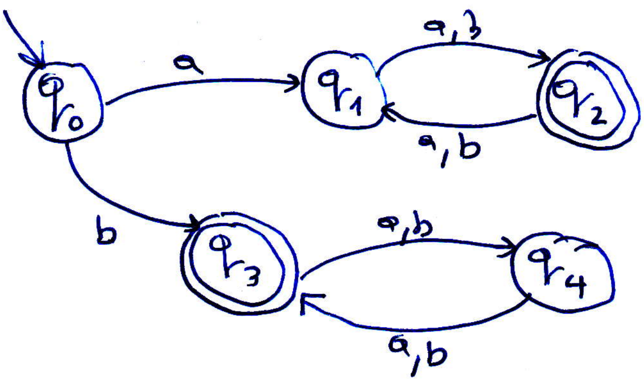
L_2:



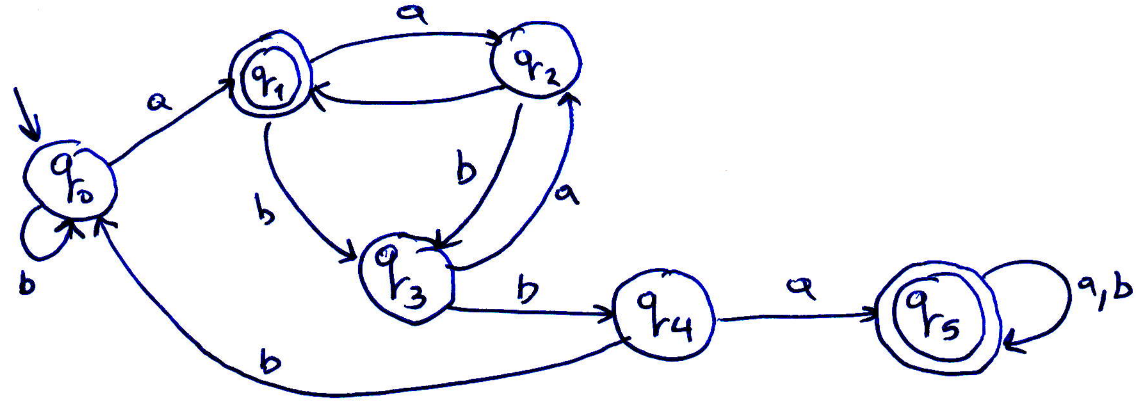
L_3:



L_4:



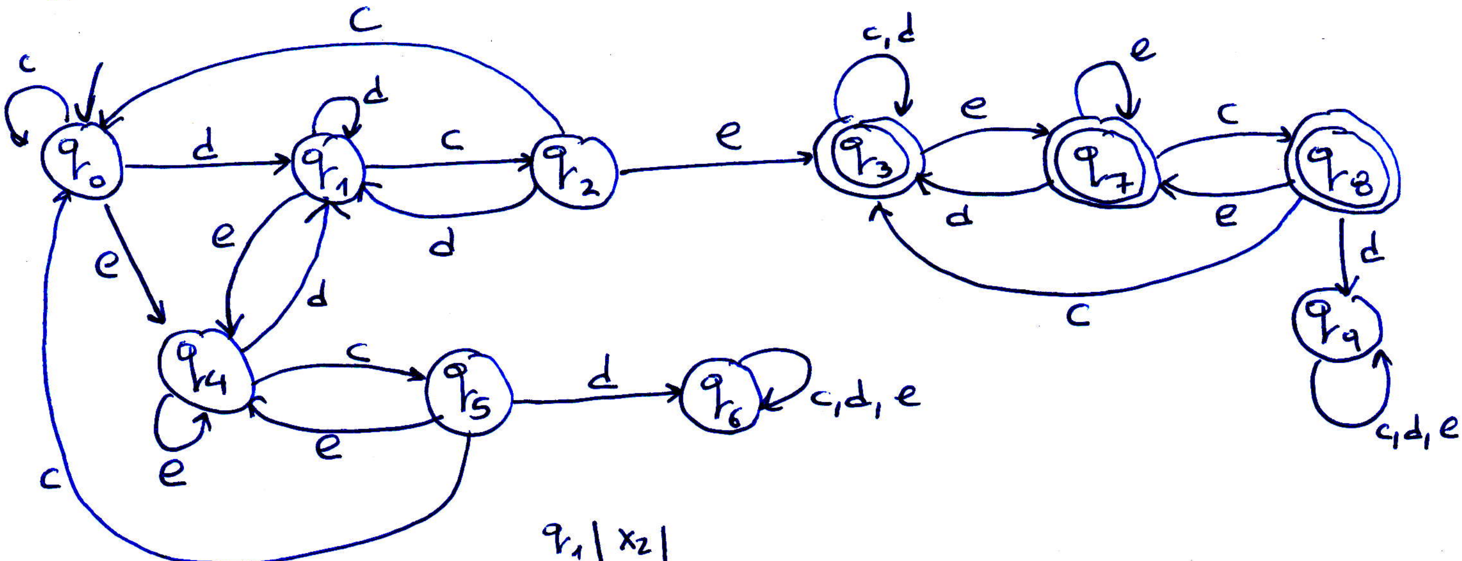
ii) L_1:



q_1	X_0				
q_2	X_2	X_0			
q_3	X_1	X_0	X_1		
q_4	X_2	X_0	X_2	X_1	
q_5	X_0	X_1	X_0	X_0	X_0
	q_0	q_1	q_2	q_3	q_4

Άρα, ελάχιστο DFA

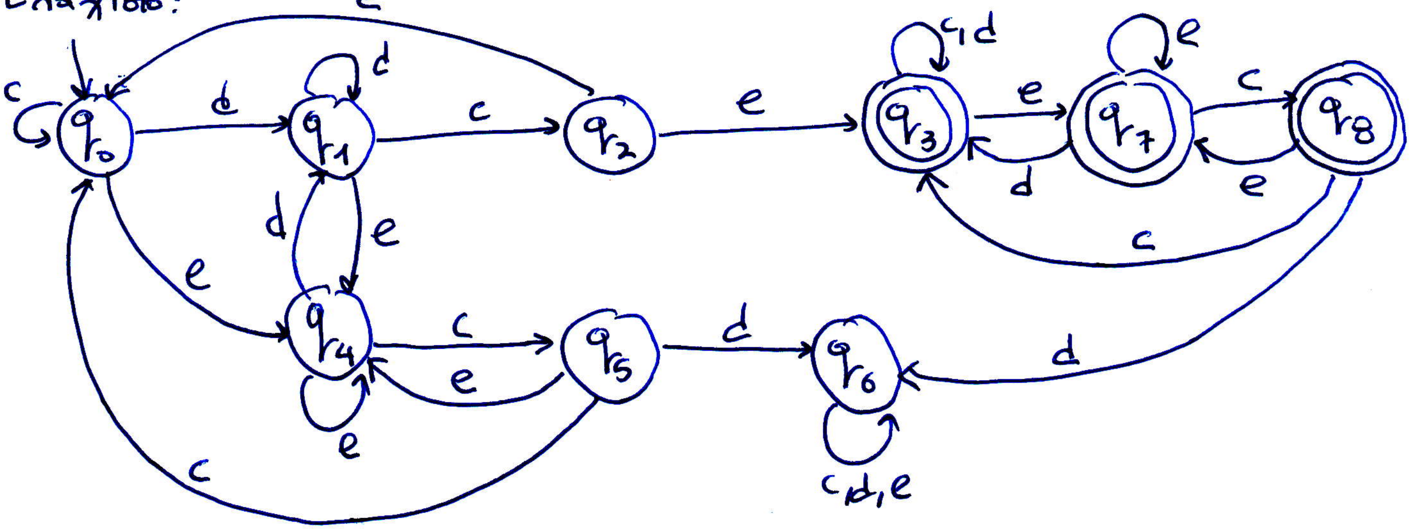
L_2:



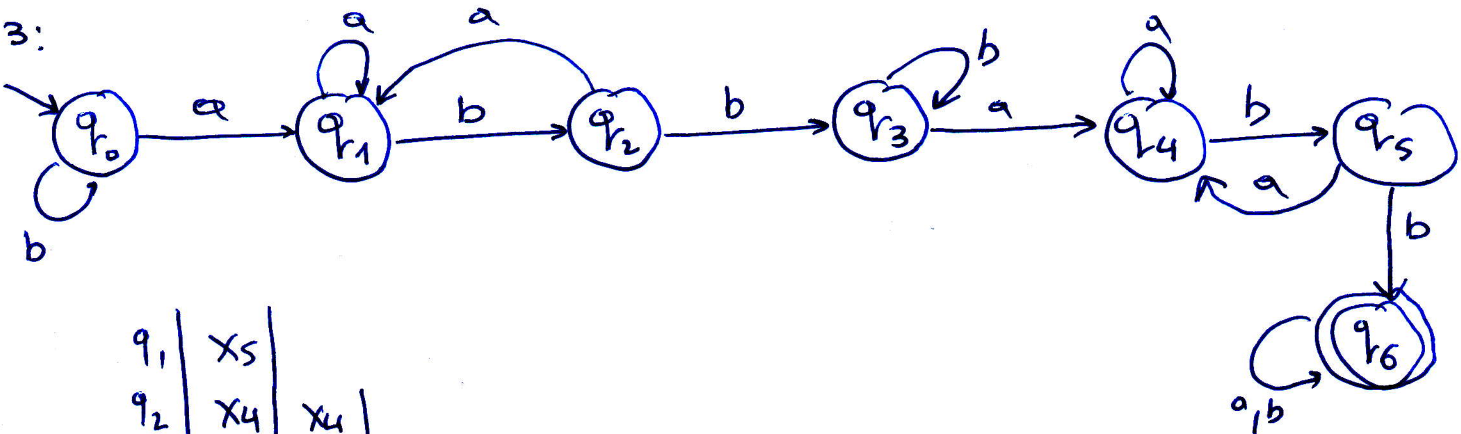
q_1	X_2								
q_2	X_1	X_1							
q_3	X_0	X_0	X_0						
q_4	X_4	X_2	X_1	X_0					
q_5	X_3	X_2	X_1	X_0	X_3				
q_6	X_3	X_2	X_1	X_0	X_3	X_4			
q_7	X_0	X_0	X_0	X_2	X_0	X_0	X_0		
q_8	X_0	X_0	X_0	X_1	X_0	X_0	X_0	X_1	
q_9	X_3	X_1	X_1	X_0	X_3	X_4		X_0	X_0
	q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8

Είναι ελάχιστο όταν συγχωνεύσουμε την κατάσταση $q_6 \equiv q_9$

Ελάχιστο:



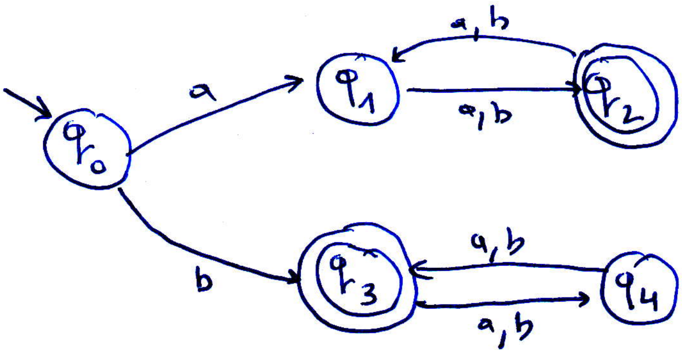
L3:



q_1	X_5					
q_2	X_4	X_4				
q_3	X_3	X_3	X_3			
q_4	X_2	X_2	X_2	X_2		
q_5	X_1	X_1	X_1	X_1	X_1	
q_6	X_0	X_0	X_0	X_0	X_0	X_0
	q_0	q_1	q_2	q_3	q_4	q_5

Είναι το ελάχιστο DFA

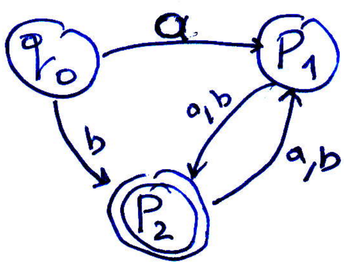
L4:



q_1	X_1			
q_2	X_0	X_0		
q_3	X_0	X_0		
q_4	X_1		X_0	X_0
	q_0	q_1	q_2	q_3

Άρα $q_1 \equiv q_4 = P_1$, $q_2 \equiv q_3 = P_2$

Ελάχιστο:



iii)

L_1: $r = b^*a(ab^*a)^*b^* + (a+b)^* abba (a+b)^*$

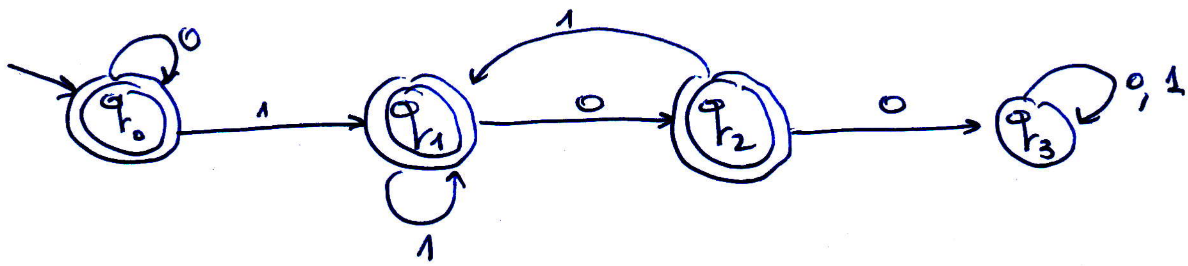
L_2: $(c + ee^*c + d(d+cd)^*(ee^*c+cc))^* d(d+cd)^* ce$
$((d+c+ee^*c)^* + (d+c+ee^*c)^* ee^*)$ (?)

L_3: $b^*a(a^*+ba)^* bbb^*a(a^*+ba)^* bb(a+b)^*$

L_4: $a(a+b)((a+b)(a+b))^* + b((a+b)(a+b))^*$

<u>Άσκηση 6</u>

a)



$q_0 = \varepsilon + q_0 0 \longrightarrow q_0 = \varepsilon 0^* = 0^*$

Arden's Theorem:
$R = Q + RP$
$R = QP^*$

$q_1 = q_0 1 + q_1 1 + q_2 1$

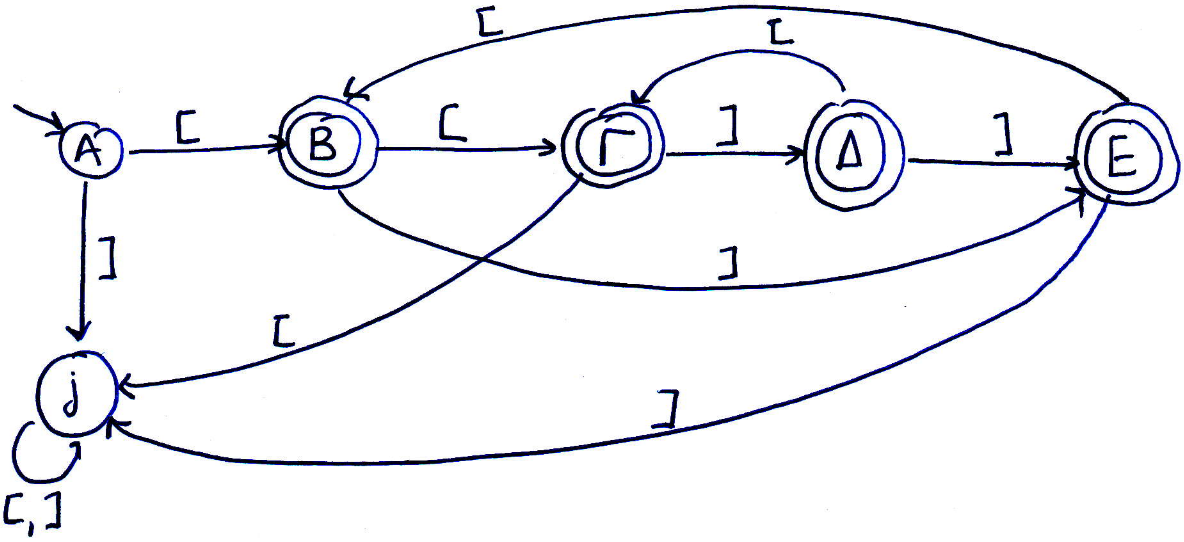
$q_2 = q_1 0$

$q_1 = 0^*1 + q_1 1 + q_1 01 = 0^*1 + q_1(1+01)$
$\Rightarrow q_1 = 0^*1(1+01)^*$

$q_2 = 0^*1(1+01)^*0$

$Z = q_0 + q_1 + q_2 = 0^* + 0^*1(1+01)^* + 0^*1(1+01)^*0$

β)



$A = \varepsilon$

$B = A[+ E[\quad \rightsquigarrow \quad B = [+ B\{] + [(][)^*]] \}[$

$\qquad\qquad\qquad\qquad B = [(( ] + [(][)^*]]) [ )^*$

$\Gamma = B[+ \Delta[$

$\Delta = \Gamma]$

$E = B] + \Delta]$

$B = [+ (B] + \Delta])[$

$B = [+ (B] + \Gamma]])[$

$\Gamma = B[+ \Gamma][\quad \rightsquigarrow \quad \Gamma = B[(][)^*$

$E = B] + \Gamma]] \quad = B] + B[(][)^*]]$

$E = B\{] + [(][)^*]] \}$

$A = B + \Gamma + \Delta + E =$

$= B + B[(][)^* + B[(][)^*] + B\{] + [(][)^*]] \}$

$= B(\varepsilon + [(][)^* + [(][)^*] + \{] + [(][)^*]] \})$

όπου $B = [(( ] + [(][)^*]]) [ )^*$

Άσκηση 7

$L = \{ z \mid z = ([^{i} ([])^{*}]^{i})^{*} \}$

Έστω κανονική γλώσσα:

Υπάρχει $n \in N$ (n = πλήθος καταστάσεων DFA). $\forall n \in N$

Επιλέγουμε $z \in L$ με μήκος $|z| \geq n$ να

PL: υπάρχει σπάσιμο $z = uvw$ με $|uv| \leq n$ $|v| \geq 0$

Για κάθε σπάσιμο $z = uvw$ με $|uv| \leq n$ και $|v| \geq 0$

Επιλέγουμε $i = 2$

$v = [^{2k}$

$z = [^{n} ([])^{*}]^{n}$

$u = [^{n-k}$

$v = [^{k}$

$w = ([])^{*}]^{n}$

Άρα $uv^{2}w \notin L$

Άρα η L όχι κανονική

Το αυτόματο που θα δεχόταν τη γλώσσα θα ήταν ένα PDA.

push(a) στην στοίβα για κάθε [στην είσοδο

pop(a) από την στοίβα για κάθε] στην έξοδο

Αποδοχή η κενή στοίβα.

* Εφόσον στοίβα κενή και στην είσοδο] τότε η λέξη θα απορρίπτεται.

$G: V = \{S\}, \; T = \{ [,] \}, \; P = \{ S \to \varepsilon, \; S \to [S], \; S \to S^{*}S \}$