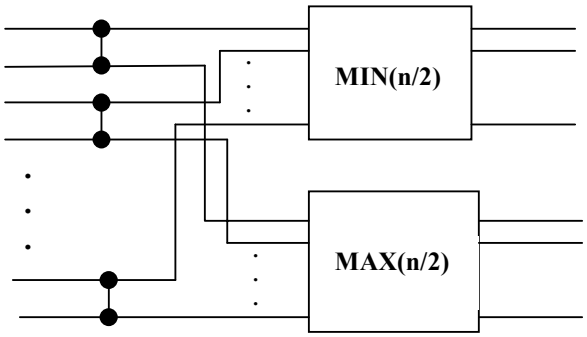
Κατ'οίκον Εργασία 4 – Σκελετοί Λύσεων

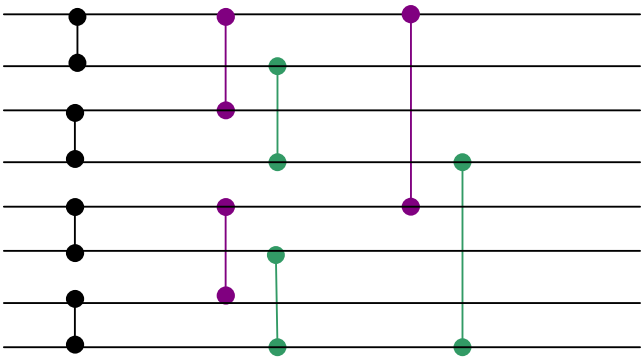
1. (α) Υποθέτουμε ότι το n είναι δύναμη του 2. Το δίκτυο βρίσκει το μέγιστο και το ελάχιστο στοιχείο του δεδομένου εισόδου ως εξής: Στην πρώτη φάση n/2 συγκριτές συγκρίνουν ταυτόχρονα ζεύγη στοιχείων (2i+1, 2i+2) για $0 \le i \le n/2-1$, δηλαδή το πρώτο με το δεύτερο, το τρίτο με το τέταρτο, και ούτω καθεξής. Τα ελάχιστα στοιχεία των συγκρίσεων περνιούνται σε ένα δίκτυο εύρεσης ελαχίστου στοιχείου ενώ τα μέγιστα σε ένα δίκτυο εύρεσης μέγιστου στοιχείου.



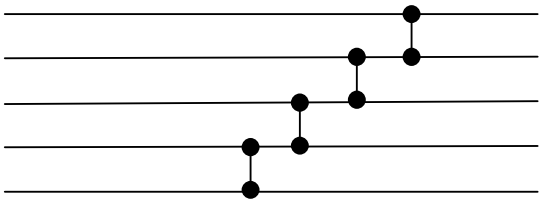
Το δίκτυο MIN(n) (αντίστοιχα MAX(n)) ορίζεται αναδρομικά ως εξής: αρχικά n/2 συγκριτές συγκρίνουν το δεδομένο εισόδου ανά δυάδες και στη συνέχεια τα ελάχιστα (μέγιστα) στοιχεία περνιούνται στο δίκτυο MIN(n/2) (αντίστοιχα MAX(n/2)).

Το βάθος ενός δικτύου MIN(n) (MAX(n)) δίνεται αναδρομικά ως εξής:
$T(n) = T(n/2) + 1 = T(n/4) + 2 = \ldots = \lg n$
και το βάθος του προτεινόμενου δικτύου $1 + \lg(n/2) = \lg n$.

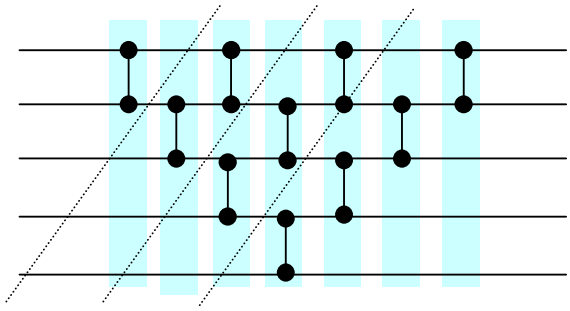
Πιο κάτω φαίνεται το ζητούμενο δίκτυο για n=8.



(β) Το πιο κάτω βασικό συγκρότημα, υποθέτοντας ότι τα στοιχεία των πρώτων n-1 εισόδων είναι ταξινομημένα, τοποθετεί το τελευταίο στοιχείο στην κατάλληλη θέση, δημιουργώντας ένα ταξινομημένο σύνολο.



Για να φτιάξουμε το ζητούμενο δίκτυο χρησιμοποιούμε το πιο πάνω συγκρότημα, για να δημιουργήσουμε αρχικά ταξινομημένη μορφή των δύο πρώτων στοιχείων, στη συνέχεια των τριών πρώτων στοιχείων, των τεσσάρων πρώτων στοιχείων και ούτω καθεξής. Γραφικά για n=5



Το βάθος του δικτύου είναι 2n-3: αφού εκτελεσθούν η πρώτη και η δεύτερη φάση σειριακά, στη συνέχεια κάθε μια από τις n-3 επόμενες φάσεις απαιτούν δύο επιπλέον μονάδες χρόνου η κάθε μια, γιατί τα υπόλοιπα βήματα κάθε φάσης μπορούν να γίνουν παράλληλα με την προηγούμενη φάση. Επομένως 3 + 2(n-3) = 2n – 3.

2. (α) Δεδομένο Εισόδου: Ένας κατευθυνόμενος γράφος G, που δεν περιέχει κύκλους αρνητικού κόστους.

Δεδομένο Εξόδου: Το κόστος του βραχύτερου μονοπατιού D[i, j] ανάμεσα σε κάθε ζεύγος κορυφών i και j.

Αρχικά θεωρείστε τον πιο κάτω ακολουθιακό κώδικα:

```
For i = 1 to n do
  For j = 1 to n do
       D[i,j] = weight of edge (i, j)

  Repeat log n times
       For i = 1 to n do
            For j = 1 to n do
                 For m = 1 to n do
                D[i,j]=min{D[i,j], D[i,m]+D[m,j]}
```

Η ορθότητα της πιο πάνω διαδικασίας μπορεί να δειχθεί από την πιο κάτω πρόταση: Μετά από την t-οστή επανάληψη του βρόχου repeat, για κάθε i, j έχουμε ότι το D[i,j] ισούται με το κόστος του βραχύτερου μονοπατιού μεταξύ των κορυφών i και j που περιέχει το πολύ 2^t ακμές. Παρατηρούμε ότι ο βρόχος αυτός δεν μπορεί να παραλληλοποιηθεί. Οι τρεις εσωτερικοί βρόχοι όμως μπορούν να εκτελεσθούν παράλληλα ως εξής:

```
For all i,j in parallel
        D[i,j] = weight of edge (i, j)

Repeat log n times
   For all i,j,m in parallel
       T[i,m, j]=min{D[i,j], D[i,m]+D[m,j]}
         D[i,j]=min{T[i,1,j] ... T[i,n,j]}
```

Χρόνος Εκτέλεσης: $\log^2 n$ (το min{T[i,1,j] ... T[i,n,j]}μπορεί να βρεθεί από ένα παράλληλο αλγόριθμο σε χρόνο log n, δες Φροντιστήριο 10, Άσκηση 1).

(β) Η βασική ιδέα του αλγορίθμου είναι η ίδια με τον αλγόριθμο από τις διαλέξεις: υπολογίζουμε τα n^3 γινόμενα και μετά προσθέτουμε τα κατάλληλα γινόμενα για να δημιουργηθούν οι θέσεις του τελικού πίνακα. Αφού όμως τώρα έχουμε μόνο $n^3/\lg n$ στη διάθεσή μας οι δύο φάσεις θα υπολογισθούν ως εξής:
Βήμα 1: ανάθεσε στους $n^3/\lg n$ υπολογιστές τα πρώτα $n^3/\lg n$ γινόμενα.
Βήμα 2: ανάθεσε στους $n^3/\lg n$ υπολογιστές τα επόμενα $n^3/\lg n$ γινόμενα.
…
Βήμα lg n: ανάθεσε στους $n^3/\lg n$ υπολογιστές τα τελευταία $n^3/\lg n$ γινόμενα.

Ανάθεσε σε κάθε ένα από τα n^2 αθροίσματα n/log n υπολογιστές (με αυτό τον τρόπο και οι $n^3/\lg n$ υπολογιστές χρησιμοποιούνται). Εκτέλεσε παράλληλα τα n^2 αθροίσματα με παραλληγή του αλγόριθμου Φροντιστήριο 10, Άσκηση 1, σε χρόνο lg n.

Συνολικός χρόνος εκτέλεσης $\Theta(\lg n)$.

3. Εξ'ορισμού το ελάχιστο κοινό πολλαπλάσιο lcm(a, b) δύο αριθμών a και b είναι ο ελάχιστος αριθμός τέτοιος ώστε
   $$lcd(a,b) = x\cdot a,\ lcd(a,b) = y\cdot b$$
   Για να υπολογίσουμε το lcd(a,b) πρέπει να βρούμε τις ελάχιστες τιμές x και y που ικανοποιούν τις πιο πάνω σχέσεις. Έστω
   $$a = gcd(a,b)\cdot\alpha,\ b= gcd(a,b)\cdot\beta$$
   όπου οι α και β είναι σχετικά πρώτοι ακέραιοι.
   Τότε
   $$lcd(a,b) = x\cdot gcd(a,b)\cdot\alpha = y\cdot gcd(a,b)\cdot\beta$$
   και
   $$x\cdot\alpha = y\cdot\beta$$

Αφού οι α και β είναι σχετικά πρώτοι μεταξύ τους έχουμε ότι α|y και β|x και οι ελάχιστες τιμές των x και y που ικανοποιούν το ζητούμενο είναι y = α και x = β.
Επομένως lcd(a,b) = a·b/gcd(a,b).

Επίσης, μπορούμε να αποδείξουμε επαγωγικά ότι

$$lcd(a_1, a_2, \ldots, a_n) = lcd(a_1, lcd(a_2, \ldots, a_n))$$

Αυτές οι δύο σχέσεις δίνουν τον πιο κάτω αναδρομικό αλγόριθμο για υπολογισμό του ελάχιστου κοινού πολλαπλασίου μιας πλειάδας ακεραίων.

```
LCD(a[], n){
   if n = 2
        g = Euclic_GCD(a[1], a[2]);
        return a[1]·a[2]/g;
   if n>2
        return LCD(a[n], LCD(a[], n-1);
}
```

4. (α) Έχουμε

$$n = p \cdot q = 863 \cdot 877 = 756851$$

Επομένως $\varphi(n) = 862 \cdot 876 = 755112$.
Θέλουμε να υπολογίσουμε το πολλαπλασιαστικό αντίστροφο του 5 modulo 755112, δηλαδή να λύσουμε την εξίσωση $5 \cdot d \equiv 1 \bmod 755112$. Αφού ΜΚΔ(5,755112)=1 η εξίσωση έχει ακριβώς μια λύση, την

$$d = x \bmod 755112 \text{ όπου } 1 = 5 \cdot x + 755112 \cdot y.$$

Χρησιμοποιώντας τον Γενικευμένο Αλγόριθμο του Ευκλείδη βρίσκουμε ότι

$$x = 302045 \text{ και } y = -2.$$

Έτσι $d = 302045 \bmod 755112 = 302045$.

(β) ALGORITHM $\leftrightarrow$ 001106 141708 190712

$$\rightarrow (001106)^5 \bmod n \; (141708)^5 \bmod n \; (190712)^5 \bmod n$$

$$= 242459\ 409188\ 167752$$