

# Μάθημα 2

## Η μέθοδος Sturm

Το θεώρημα του Sturm μας δίνει έναν τρόπο καταμέτρησης των πραγματικών ριζών ενός πολυωνύμου σε δοσμένο διάστημα που τηρεί κάποιες συνθήκες. Εισάγουμε την έννοια της ακολουθίας Sturm ενός πολυωνύμου, αποδεικνύουμε το σχετικό θεώρημα και κατόπιν δίνουμε αλγόριθμο εντοπισμού των πραγματικών ριζών.

### 2.1 Ακολουθίες Sturm

Έστω μια ακολουθία τιμών  $(t_1, \dots, t_k)$ . Ορίζουμε ως το πλήθος μεταβολών προσήμου το πλήθος μεταβολών στην ακολουθία μη-μηδενικών προσήμων. Π.χ. πλήθος μεταβολών της  $[-, +, +, -] = 2$ , πλήθος μεταβολών της  $[+, 0, +, -] = 1$ .

Έστω  $a \in \mathbb{R} \cup \{-\infty, +\infty\}$  και μια ακολουθία πολυωνύμων  $(p_1, \dots, p_k)$ . Ορίζουμε ως το πλήθος μεταβολών προσήμου της ακολουθίας στο σημείο  $a$ , και το συμβολίζουμε  $V(a)$ , το πλήθος μεταβολών προσήμου στην ακολουθία των τιμών  $[p_1(a), \dots, p_k(a)]$ , όπου  $p(\pm\infty) = \lim_{x \rightarrow \pm\infty} p(x)$ .

**Ορισμός 2.1.1.** Μια ακολουθία Sturm ενός πολυωνύμου  $p \in K[x]$  στο  $[a, b] \subset K \cup \{-\infty, +\infty\}$ , όπου  $K$  κλειστό πραγματικό, είναι μια ακολουθία  $(p_1, p_2, \dots, p_k)$  με  $p_1 = p$  εάν:

1.  $p(a)p(b) \neq 0$ ,
2.  $\forall c \in [a, b], p_k(c) \neq 0$ ,
3.  $\forall c \in [a, b] : p_j(c) = 0 \Rightarrow p_{j-1}(c)p_{j+1}(c) < 0, \quad j \in \{2, \dots, k-1\}$
4.  $\forall c \in [a, b] : p_1(c) = 0 \Rightarrow$  υπάρχουν διαστήματα  $[c_1, c), (c, c_2]$  τέτοια ώστε:  $u_1 \in [c_1, c) \Rightarrow p_1(u_1)p_2(u_1) < 0$  και  $u_2 \in (c, c_2] \Rightarrow p_1(u_2)p_2(u_2) > 0$ .

Το επόμενο θεώρημα δείχνει πως ο παραπάνω ορισμός δεν είναι κενός, δηλ. υπάρχει τουλάχιστον μια ακολουθία Sturm. Το θεώρημα ορίζει έτσι την απλή ακολουθία Sturm.

**Θεώρημα 2.1.1** (Υπαρξη ακολουθίας Sturm). Έστω μια ακολουθία  $(p_1, p_2, \dots, p_k)$  με  $p_1 = p \in K[x]$  ένα πολυώνυμο χωρίς τετράγωνα και  $K$  κλειστό πραγματικό,  $p_2 = p'$  (παράγωγος) και για  $i = 3, \dots, k, p_i = -(p_{i-2} \bmod p_{i-1})$ . Η ακολουθία  $(p_i)$  είναι ακολουθία Sturm σε διάστημα  $[a, b]$  όπου  $p(a)p(b) \neq 0$  και καλείται απλή ακολουθία Sturm.

Απόδειξη. (1) Κατ' επιλογή τα  $a, b$  δεν είναι ρίζες του  $p$ .

(2)  $\text{MK}\Delta(p, p') =$  μη μηδενική σταθερά διότι το  $p$  δεν έχει τετράγωνα. Το  $p_k$  είναι πολλαπλάσιο του  $\text{MK}\Delta(p, p')$  επί μια μη μηδενική σταθερά άρα  $p_k =$  σταθερά. Εδώ χρησιμοποιείται η υπόθεση πως το πολυώνυμο είναι χωρίς τετράγωνα.

(3)  $\exists q_i \in K[x] : p_{i-1} = p_i q_i - p_{i+1} \Rightarrow p_{i-1}(c) = 0 - p_{i+1}(c)$ . Εάν  $p_{i-1}(c) = 0 = p_{i+1}(c)$  τότε  $\forall j > i - 2, p_j(c) = 0$ : άτοπο για  $j = k$ .

(4) Για  $c$  τέτοιο ώστε  $p(c) = 0$  έχουμε  $p'(c) \neq 0$  (διότι  $p$  χωρίς τετράγωνα) άρα υπάρχει διάστημα  $(c_1, c_2)$  που περιέχει το  $c$  όπου το  $p'$  έχει σταθερό πρόσημο ενώ το  $p$  αλλάζει πρόσημο στο  $c$ , δεδομένου ότι πρόκειται για απλή ρίζα.  $\square$

**Πόρισμα 2.1.1.** Κάθε ακολουθία  $(p_i) = (p, p', \dots)$  όπου  $a_i p_i = b_i p_{i-2} + p_{i-1} q_{i+1}$  για  $a_i, b_i \in K, a_i b_i < 0$ , όπου το  $p(x) \in K[x]$  είναι χωρίς τετράγωνα και το  $K$  κλειστό πραγματικό, είναι ακολουθία Sturm στο  $[a, b]$  όπου  $p(a)p(b) \neq 0$ .

Απόδειξη. Όπως παραπάνω: άσκηση.  $\square$

**Λήμμα 2.1.1.** Μία ακολουθία προσήμων  $(\sigma, \tau, -\sigma)$  έχει 1 αλλαγή προσήμου για κάθε  $\sigma, \tau \in \{+, -\}$ .

## 2.2 Το Θεώρημα Sturm

Είμαστε τώρα έτοιμοι να διατυπώσουμε το βασικό θεώρημα της ενότητας, που θα μας επιτρέψει να μετράμε τις διαφορετικές πραγματικές ρίζες ενός πολυωνύμου σε ένα διάστημα, χωρίς όμως να υπολογίζουμε τις πολλαπλότητές τους.

**Θεώρημα 2.2.1** (Sturm). Έστω μια ακολουθία Sturm  $(p_i) = (p_1, \dots, p_k)$  στο  $[a, b] \subset K \cup \{-\infty, +\infty\}$ , όπου  $p = p_1 \in K[x]$  και  $K$  κλειστό πραγματικό. Το πλήθος των διαφορετικών πραγματικών ριζών του  $p_1(x)$  στο  $[a, b]$  ισούται με  $V(a) - V(b)$ , όπου  $V(\cdot)$  το πλήθος μεταβολών προσήμου της  $(p_i)$ .

*Απόδειξη.* Έστω  $a_1 < \dots < a_m$  οι ρίζες  $\in (a, b)$  ΌΛΩΝ των πολυωνύμων στην  $(p_i)$ , δηλαδή όλες οι τιμές στο διάστημα στις οποίες κάποιο πολυώνυμο της ακολουθίας μηδενίζεται. Θα αποδείξουμε επαγωγικά πως η διαφορά  $V(a) - V(c_i)$  ισούται με το πλήθος των πραγματικών ριζών στο  $(a, c_i)$  για τυχαίο  $c_i \in (a_i, a_{i+1})$ ,  $i = 0, \dots, m$ , όπου  $a_0 = a, a_{m+1} = b$ .

Βάση της επαγωγής: Έστω  $c_0 \in (a_0, a_1)$ . Αν  $p_i(a_0) \neq 0$ ,  $i = 2, \dots, k-1$  τότε προφανώς από το θεώρημα μέσης τιμής του Bolzano σε ένα διάστημα  $(a_0 - \varepsilon, c_0)$ , για κάποιο  $\varepsilon > 0$ , κάθε πολυώνυμο διατηρεί το πρόσημό του, δηλαδή  $V(a) = V(c_0) \Rightarrow V(a) - V(c_0) = 0$ .

Ακόμη κι αν υπάρχει  $i \in \{2, \dots, k-1\}$  με  $p_i(a) = 0$ , η ιδιότητα (3) της ακολουθίας Sturm δίνει  $p_{i-1}(a)p_{i+1}(a) < 0$ , άρα η τριάδα συνεισφέρει στο  $V(a)$  κατά 1, επειδή η ακολουθία προσήμων είναι της μορφής  $[\dots, \sigma, 0, -\sigma, \dots]$ ,  $\sigma, \tau \in \{+, -\}$  στις θέσεις  $i-1, i, i+1$ . Καθώς στο διάστημα  $(a, c_0)$  δεν υπάρχουν ρίζες, η ακολουθία προσήμων στο  $c_0$  είναι της μορφής  $[\dots, \sigma, \tau, -\sigma, \dots]$  στις ίδιες θέσεις, άρα σύμφωνα με το Λήμμα 2.1.1 συνεισφέρει στο  $V(c_0)$  κατά 1. Αν υπάρχει κι άλλος τέτοιος δείκτης  $i$ , με το ίδιο επιχείρημα φθάνουμε στην ίδια μεταβολή των αλλαγών προσήμου, άρα τελικά  $V(a) - V(c_0) = 0$ .

Επαγωγικό βήμα: Υποθέτοντας  $V(a) - V(c_i) = \text{πλήθος ριζών} \in (a, c_i)$  θα το αποδείξουμε για  $c_{i+1}$  όπου  $c_i < a_{i+1} < c_{i+1} < a_{i+2}$ . Διακρίνουμε δυο περιπτώσεις ανάλογα με το αν  $p(a_{i+1}) \neq 0$  ή  $p(a_{i+1}) = 0$ :

1. Έστω  $p(a_{i+1}) \neq 0$ . Τότε  $p_j(a_{i+1}) = 0$ , για κάποιο  $j \in \{2, \dots, k-1\}$ . Χάριν της ιδιότητας (3) των ακολουθιών Sturm,  $p_{j+1}(a_{i+1})p_{j-1}(a_{i+1}) < 0$ , συνεπώς έχουμε τις ακολουθίες προσήμων

$$\begin{aligned} [p_{j-1}(c_i), p_j(c_i), p_{j+1}(c_i)] &= [\sigma, \tau_0, -\sigma], \\ [p_{j-1}(c_{i+1}), p_j(c_{i+1}), p_{j+1}(c_{i+1})] &= [\sigma, \tau_1, -\sigma] \end{aligned}$$

για  $\sigma, \tau_0, \tau_1 \in \{+, -\}$ . Σύμφωνα με το Λήμμα 2.1.1, υπάρχει ακριβώς μία αλλαγή προσήμου σε καθεμιά από τις 2 ακολουθίες. Άρα, αν μόνο το  $p_j$  μηδενίζεται στο  $a_{i+1}$ , έχουμε  $V(c_{i+1}) = V(c_i)$ . Αν υπάρχει κι άλλο πολυώνυμο που μηδενίζεται στο  $a_{i+1}$  το ίδιο επιχείρημα δείχνει πως τελικά  $V(c_{i+1}) = V(c_i)$ .

Αφού οι ρίζες του  $p$  δεν αυξηθήκαν στο διάστημα  $(c_i, c_{i+1})$ , ο ισχυρισμός αποδείχθηκε.

2. Έστω  $p(a_{i+1}) = 0$ . Χάριν της ιδιότητας (4) των ακολουθιών Sturm, τα  $p_1, p_2$  έχουν διαφορετικό πρόσημο στο  $c_i$  και το ίδιο στο  $c_{i+1}$ . Επίσης, από την ιδιότητα (3) για  $j = 2$ , έχουμε  $p_2(a_{i+1}) = 0 \Rightarrow p_1(a_{i+1}) \neq 0$ , το οποίο είναι άτοπο. Άρα από θ. Bolzano το  $p_2$  διατηρεί το πρόσημό του στο  $(a_i, a_{i+2})$ , δηλαδή οι ακολουθίες προσήμων στα  $c_i$  και  $c_{i+1}$  είναι:

$$\begin{aligned} [p_1(c_i), p_2(c_i), \dots] &= [-\rho, \rho, \dots], \\ [p_1(c_{i+1}), p_2(c_{i+1}), \dots] &= [\rho, \rho, \dots] \end{aligned}$$

όπου  $\rho \in \{+, -\}$ .

Αν κανένα άλλο πολυώνυμο με δείκτη  $j > 2$  δε μηδενίζεται στο  $a_{i+1}$  βλέπουμε ότι  $V(c_{i+1}) = V(c_i) - 1$ .

Αν τώρα για  $j > 2$ , υπάρχει  $p_j$  με  $p_j(a_{i+1}) = 0$  ακολουθούμε ακριβώς την ίδια διαδικασία όπως στην περίπτωση 1 πιο πάνω, για να δείξουμε ότι για την υπακολουθία  $[p_2, p_3, \dots, p_k]$  είναι  $V^*(c_{i+1}) = V^*(c_i)$ , δηλαδή ισχύει και πάλι  $V(c_{i+1}) = V(c_i) - 1$ .

Τελικά βλέπουμε ότι  $V(a) - V(c_{i+1}) = V(a) - V(c_i) + 1$  άρα από επαγωγική υπόθεση φθάνουμε στο ζητούμενο (δεδομένου ότι οι ρίζες του  $p$  έχουν αυξηθεί κατά μία στο διάστημα  $(c_i, c_{i+1})$ ).

□

**Άσκηση 2.2.1.** Η έννοια της ακολουθίας Sturm γενικεύεται με το να αναιρέσουμε την προϋπόθεση (1) του ορισμού 2.1.1. Τότε τα διαστήματα στην προϋπόθεση (4) πρέπει να ανήκουν στο διάστημα  $[a, b]$ , δηλ. η προϋπόθεση (4) απλοποιείται στην περίπτωση που  $c = a$  ή  $c = b$ . Αποδείξτε πως το θεώρημα 2.2.1 ισχύει.

Στόχος είναι η απομόνωση όλων των ριζών δηλ. ο υπολογισμός ρητών διαστημάτων που καθένα περιέχει μια μοναδική ρίζα. Περιορίζουμε το διάστημα όπου βρίσκονται οι (πραγματικές) ρίζες του  $p(x)$  χρησιμοποιώντας το θεώρημα 1.4.1 και το πόρισμά του.

**Παράδειγμα 2.2.1.** Δίνεται  $p = x^3 + 2x - 3 = (x - 1)(x + 1/2 + i\sqrt{11/2})(x + 1/2 - i\sqrt{11/2})$ . Ακολουθία Sturm:

$$p_1 = p, p_2 = p' = 3x^2 + 2, p_3 = -(p_1 \bmod p_2) = -(4/3)x + 3, p_4 = -(p_2 \bmod p_3) = -275/16.$$

Στο παράδειγμα 1.4.1 υπολογίστηκε το αρχικό διάστημα (0.7211, 2.45), το οποίο περιέχει όλες τις ρίζες του  $p$ . Προκύπτει λοιπόν ο παρακάτω πίνακας, όπου μετά το αρχικό διάστημα (0, 3) επελέγησαν τα σημεία 3/2, 3/4, 9/8 με αυτή τη σειρά.

$a =$	0	3/4	1	9/8	3/2	3
$p_1(a)$	-	-	0	+	+	+
$p_2(a)$	+	+	+	+	+	+
$p_3(a)$	+	+	+	+	+	-
$p_4(a)$	-	-	-	-	-	-
$V(a) =$	2	2	1	1	1	1

**Άσκηση 2.2.2.** Έστω πολυώνυμο  $f = x^3 - 13x + 12$ . Δίνεται η ταυτότητα  $f'(x = 18/13) = -1225/169$ . Υπολογίστε μια ακολουθία Sturm και απομονώστε τις ρίζες.

Απάντηση:  $p_1 = f, p_2 = f' = 3x^2 - 13, p_3 = 26x/3 - 12, p_4 > 0$ . Ρίζες = 1, 3, 4.

## 2.3 Ο αλγόριθμος Sturm

Δίνουμε τώρα τον αλγόριθμο Sturm για εύρεση πραγματικών ριζών ενός πολυωνύμου με απλές ρίζες σε ψευδοκώδικα:

Αλγόριθμος STURM

▷ Είσοδος: Ένα πολυώνυμο  $p \in \mathbb{R}[x]$  χωρίς τετράγωνα.

▷ Έξοδος: Ένα σύνολο  $R$  με στοιχεία διαστήματα απομόνωσης των πραγματικών ριζών του  $p$ .

- 1  $I_0 \leftarrow \mathbf{Cauchy}(p)$
- 2 Υπολόγισε ακολουθία Sturm  $S = (p_1, \dots, p_k)$  στο  $I_0$
- 3  $Q \leftarrow \{I_0\}, R \leftarrow \emptyset$
- 4 **όσο**  $Q \neq \emptyset$
- 5      $I \leftarrow \mathbf{εξαγωγή}(Q)$
- 6      $roots \leftarrow \mathbf{VARS}(S, a) - \mathbf{VARS}(S, b)$
- 7     **αν**  $roots = 1, R \leftarrow R \cup I$
- 8     **αν**  $roots > 1, Q \leftarrow Q \cup \{I_L, I_R\}$
- 9 **επέστρεψε**  $R$

Όπου  $I = [a, b]$ , και συμβολίζουμε  $I_L = [a, \frac{a+b}{2}]$ ,  $I_R = [\frac{a+b}{2}, b]$ . Τα σύνολα  $Q, R$  μπορούν να υλοποιηθούν με κάποια δομή δεδομένων, πχ στοιβία ή ουρά. Η εντολή **Cauchy**( $p$ ) επιστρέφει το διάστημα  $I_0 = [-B, B]$ , όπου  $B$  το φράγμα ριζών του  $p$  από τον τύπο του Cauchy. Ο παραπάνω αλγόριθμος δεν λαμβάνει υπόψη την περίπτωση κάποιο από τα άκρα των  $I_L, I_R$  να είναι ρίζα του  $p(x)$ , όμως ένας τέτοιος έλεγχος είναι εύκολο να προστεθεί και δεν επιβαρύνει σημαντικά τον αλγόριθμο.

Δίνεται και η ρουτίνα  $\mathbf{VARS}(S, r)$ , η οποία εκτελεί την αποτίμηση της ακολουθίας Sturm σε δοσμένη τιμή και μετρά τις εναλλαγές προσήμων στην ακολουθία που προκύπτει:

Αλγόριθμος VARS

▷ Είσοδος: Μια ακολουθία πολυωνύμων  $S = (p_1, p_2, \dots, p_k)$  και μια τιμή  $r \in \mathbb{Q}$

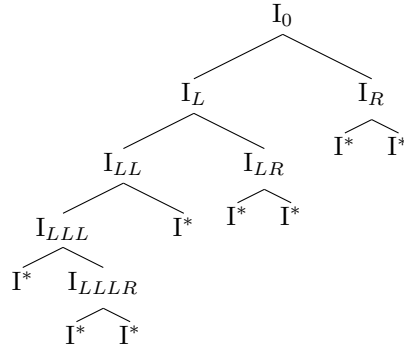
▷ Έξοδος: Το πλήθος των αλλαγών προσήμου της  $S(r) = (p_1(r), p_2(r), \dots, p_k(r))$

- 1  $V \leftarrow 0$
- 2  $\sigma \leftarrow \mathbf{πρόσημο}(p_1(r))$
- 3 **για**  $i = 2$  **μέχρι**  $k$
- 4      $\tau \leftarrow \mathbf{πρόσημο}(p_i(r))$
- 5     **αν**  $\sigma\tau = -1, V \leftarrow V + 1$
- 6     **αν**  $\tau \neq 0, \sigma \leftarrow \tau$
- 7 **επέστρεψε**  $V$

Όπου η εντολή **πρόσημο()** επιστρέφει 1 αν το όρισμα είναι θετικό, -1 αν είναι αρνητικό, ή 0 αν το όρισμα είναι το 0.

Προχωράμε στην ανάλυση του αλγορίθμου. Έστω  $d$  ο βαθμός του  $p$ ,  $p(x) = \sum_{i=0}^d c_i x^i$ , και έστω ότι οι συντελεστές του έχουν μήκος  $O_B(\tau)$ . Για την ώρα θα δεχθούμε ότι το βήμα 2 στον αλγόριθμο STURM, δηλαδή ο υπολογισμός μιας ακολουθίας Sturm<sup>1</sup>, έχει πολυπλοκότητα  $O_B^*(d^3\tau)$  και ότι οι συντελεστές κάθε πολυωνύμου  $p_i$  έχουν μήκος  $O_B(d\tau)$ . Επειδή  $B = 1 + \max_{0 \leq i \leq d} \left| \frac{c_i}{c_d} \right|$ , το  $B$  έχει μήκος  $O_B(\tau)$ , δηλαδή  $B \cong 2^\tau$ .

Οι υποδιαίρεσεις (διχοτομήσεις) διαστημάτων που γίνονται δημιουργούν ένα νοητό δυαδικό δέντρο, με φύλλα τα διαστήματα απομόνωσης των ριζών του  $p$ , τα οποία συμβολίζονται στο παρακάτω παράδειγμα με  $I^*$ .



Στο δέντρο αυτό κάθε κόμβος-διάστημα χαρακτηρίζεται από το ύψος  $h(I)$  στο οποίο βρίσκεται, και μάλιστα είναι

$$h(I) = \lg \frac{|I_0|}{|I|} \quad (2.1)$$

όπου με  $|I|$  συμβολίζουμε το μήκος του διαστήματος. Η σχέση προκύπτει άμεσα αν σκεφτούμε πως σε κάθε επίπεδο το μήκος υποδιπλασιάζεται, κι έτσι είναι  $|I| = 2^{-h(I)}|I_0|$ .

Όταν χρησιμοποιούμε κατάλληλη ακολουθία Sturm, η αποτίμησή της σε έναν ρητό με μήκος<sup>2</sup>  $O_B(\sigma)$  έχει πολυπλοκότητα  $O_B^*(d^2(\tau + \sigma))$ . Αυτή είναι και η πολυπλοκότητα της ρουτίνας VARS όταν η είσοδος είναι  $O_B(\sigma)$ , καθώς οι υπόλοιπες πράξεις μεταξύ προσήμων είναι αμελητέες. Τι μήκος έχουν όμως οι ρητοί στους οποίους εφαρμόζουμε τη ρουτίνα; Όπως φαίνεται και στο παραπάνω δέντρο, σε βάθος  $h \equiv h(I)$  τα άκρα του διαστήματος  $I$  προκύπτουν με  $h$  διαδοχικές διαιρέσεις με το 2 ποσοτήτων ανάλογων των άκρων του  $I_0$ , άρα θα έχουν μήκος  $O_B(\tau + h)$ . Έτσι τελικά η VARS τρέχει σε χρόνο  $O_B^*(d^2(\tau + h))$ .

Για να βρούμε τη συνολική πολυπλοκότητα του αλγορίθμου πρέπει να εκτιμήσουμε πόσες φορές θα εκτελεστεί η επανάληψη στα βήματα 4-8, το οποίο είναι ανάλογο του αριθμού των υποδιαίρεσεων που θα γίνουν στο διάστημα  $I$  (βήμα 8). Τέλος, ο αριθμός των επαναλήψεων θα πολλαπλασιαστεί με την πολυπλοκότητα της ρουτίνας VARS για να έχουμε το τελικό αποτέλεσμα.

Υπενθυμίζουμε το μέτρο Mahler του πολυωνύμου  $p(x)$

$$M = |c_d| \prod_{i=1}^d \max\{1, |\rho_i|\} \quad (2.2)$$

όπου  $\rho_i$ ,  $i = 1, \dots, d$  οι μιγαδικές ρίζες του  $p$ . Για το μέτρο Mahler ισχύει το φράγμα

$$M \leq \sqrt{c_0^2 + c_1^2 \dots + c_d^2} \leq 2^\tau \sqrt{d+1} \quad (2.3)$$

Για να φράξουμε το πλήθος των υποδιαίρεσεων  $C$  που εκτελεί ο αλγόριθμος χρειαζόμαστε και το παρακάτω

**Θεώρημα 2.3.1.** (Davenport-Mahler-Mignotte) Αν  $p(x) \in \mathbb{Z}[x]$  και  $\{a_1, \dots, a_k\}$ ,  $\{b_1, \dots, b_k\}$  δυο σύνολα ριζών του, με  $|a_i| > |a_{i+1}|$ ,  $|b_i| > |b_{i+1}|$  και  $|a_i| > |b_i|$  τότε ισχύει

$$\prod_{i=1}^k |a_i - b_i| \geq \frac{(\sqrt{3}/d)^k}{M^{d-1} \cdot d^{d/2}}$$

όπου  $M$  το μέτρο Mahler του  $p(x)$ .

<sup>1</sup>Η βέλτιστη αυτή τιμή επιτυγχάνεται με την ακολουθία Habicht και μπορεί να μειωθεί περισσότερο αν υπολογιστεί μια ακολουθία ηγλίκων, αντί για τα υπόλοιπα.

<sup>2</sup>δυαδικό μήκος (bit complexity) ρητού ορίζουμε τη μέγιστη τιμή από το δυαδικό μήκος του αριθμητή και του παρονομαστή του

Ας θεωρήσουμε τώρα το σύνολο  $\mathcal{S} = \{I : \text{υπάρχει ακριβώς μια ρίζα στο } I_L \text{ και ακριβώς μια στο } I_R\}$ , δηλαδή το  $\mathcal{S}$  περιέχει τα διαστήματα του δέντρου που έχουν 2 φύλλα (στο παράδειγμα είναι τα  $I_R, I_{LR}, I_{LLL}$ ). Επειδή τα φύλλα είναι το πολύ  $d$ , έχουμε ότι το πλήθος των στοιχείων του είναι

$$|\mathcal{S}| \leq \frac{d}{2} \quad (2.4)$$

Το θεώρημα (2.3.1) ισχύει για  $k = |\mathcal{S}|$  και  $a_i, b_i$  οι ρίζες στο  $I_i \in \mathcal{S}$ . Λογαριθμώντας παίρνουμε

$$-\log \prod_{i=1}^{|\mathcal{S}|} |a_i - b_i| \leq (d-1) \log M + \frac{d}{2} \log d + |\mathcal{S}| \log d - \frac{|\mathcal{S}|}{2} \log 3$$

και λαμβάνοντας υπόψιν από τις (2.3), (2.4) ότι  $\log M = O(\tau + \log d)$  και  $|\mathcal{S}| = O(d)$ , είναι τελικά

$$-\log \prod_{i=1}^{|\mathcal{S}|} |a_i - b_i| = O(d\tau + d \log d) \quad (2.5)$$

Έχοντας κατά νου όλα τα παραπάνω, μπορούμε να φράξουμε το  $C$  ως εξής:

$$\begin{aligned} C &\leq \sum_{I \in \mathcal{S}} h(I) \\ &\stackrel{(2.1)}{=} \sum_{I \in \mathcal{S}} \lg \frac{|I_0|}{|I|} \\ &= |\mathcal{S}| \lg |I_0| - \sum_{I \in \mathcal{S}} \lg |I| \\ &< |\mathcal{S}| \lg(2B) - \sum_{I \in \mathcal{S}} \lg(a_i - b_i) \\ &< |\mathcal{S}| \tau - \sum_{I \in \mathcal{S}} \log(a_i - b_i) \\ &\stackrel{(2.4)}{<} d\tau - \log \prod_{i=1}^{|\mathcal{S}|} |a_i - b_i| \\ &\stackrel{(2.5)}{<} d\tau + d\tau + d \log d \\ &= O_B(d\tau + d \log d) = O_B^*(d\tau) \end{aligned}$$

Μια παρατήρηση είναι εδώ ότι  $h \leq C$ , άρα το φράγμα για την πολυπλοκότητα της VARS είναι  $O_B^*(d^3\tau)$ . Τελικά ο αλγόριθμος έχει συνολική πολυπλοκότητα  $O_B^*(C \cdot d^3\tau) = O_B^*(d^4\tau^2)$ .