ΕΠΛ232: Ἀλγόριθμοι καὶ Πολυπλοκότητα — Μ. Μαυρονικόλας — 22/4/96

3η Σειρὰ Θεωρητικῶν Ἀσκήσεων – Μέρος Α'

-- Πρόχειρες λύσεις --

1. Συνάρτηση ΠιθανοτικήΕπιλογή (S, i)

/* $|S| = n$ καὶ $1 \leq i \leq n$ /*

- Διάλεξε ἕνα "σημεῖο" x_0 ἀπὸ τὸ σύνολο S ὁμοιόμορφα καὶ τυχαῖα
- Σχημάτισε τὰ σύνολα S_1 καὶ S_2 ὅπου: $S_1 = \{x \in S : x < x_0\}$ καὶ $S_2 = \{x \in S : x > x_0\}$.
- Ἄν $|S_1| = i-1$, ἐπίστρεψε τὸ x ἀλλοιῶς ἄν $|S_1| < i-1$ τότε ἐπίστρεψε ΠιθανοτικήΕπιλογή$(S_2, i-$
  ἀλλοιῶς ἐπίστρεψε ΠιθανοτικήΕπιλογή(S_1, i)

Ἔστω $T(n)$ ἡ ἀναμενόμενη χρονική πολυπλοκότητα τῆς συνάρτησης ΠιθανοτικήΕπιλογή. Τότε:

$$T(n) \leq \sum_{k=0}^{n-1} \text{Πιθανότητα}(|S_1| = k) \times \max\{T(k), T(n-k-1)\}$$

$$= \sum_{k=0}^{n-1} \frac{1}{n} \max\{T(k), T(n-k-1)\}$$

(λόγω ὁμοιομορφίας)

$$= \frac{1}{n} \sum_{k=0}^{n-1} \max\{T(k), T(n-k-1)\}$$

Ὑποθέτοντας ὅτι ἡ T εἶναι μονοτονικὰ μὴ φθίνουσα συνάρτηση

$$T(k) \geq T(n-k-1) \iff k \geq n-k-1 \iff k \geq \frac{n-1}{2}$$

Συνεπῶς: $$\max\{T(k), T(n-k-1)\} = \begin{cases} T(k), & k \geq (n-1)/2 \\ T(n-k-1), & k < \frac{n-1}{2} \end{cases}$$

ὁπότε ἔχουμε:

$$T(n) \leq \frac{1}{n}\left[\sum_{0 \leq k < \frac{n-1}{2}} T(n-k-1) + \sum_{\frac{n-1}{2} \leq k \leq n-1} T(k)\right]$$

$$= \frac{1}{n}\left[\sum_{\frac{n-1}{2} < k' \leq n-1} T(k') + \sum_{\frac{n-1}{2} \leq k \leq n-1} T(k)\right]$$

$$\leq \frac{1}{n}\left[\sum_{\frac{n-1}{2} \leq k' \leq n-1} T(k') + \sum_{\frac{n-1}{2} \leq k \leq n-1} T(k)\right]$$

$$= \frac{2}{n} \sum_{\frac{n-1}{2} \leq k \leq n-1} T(k)$$

Δείχνουμε μέ έπαγωγή ότι $T(n) \in O(n)$, δηλ. $T(n) \leq c$ γιά κάθε $n \geq 0$, όπου $c > 0$. Ἡ βάση της έπαγωγης είνα προφανής. Ὑποθέτουμε έπαγωγικά ότι $T(n') \leq cn'$ γιά κάθε n' τέτοιο ὥστε $0 \leq n' < n$. Θά δείξουμε, στό έπαγωγικό βήμα, ότι $T(n) \leq cn$. Ἔχουμε:

$$T(n) \leq \frac{2}{n} \sum_{\frac{n-1}{2} \leq k \leq n-1} ck$$

$$= \frac{2c}{n} \sum_{\frac{n-1}{2} \leq k \leq n-1} k$$

$$= \frac{2c}{n}\left[\sum_{0 \leq k \leq n-1} k - \sum_{0 \leq n \leq \frac{n-1}{2}-1} k\right]$$

$$= \frac{2c}{n}\left[\frac{(n-1)n}{2} - \frac{\left(\frac{n-1}{2}-1\right)\cdot\left(\frac{n-1}{2}\right)}{2}\right]$$

$$= \frac{2c}{n}\left(\frac{n^2}{4}-\frac{3}{8}\right) \leq \frac{2c}{n}\cdot\frac{n^2}{4} = \frac{cn}{2} \leq cn,$$

ὅπως χρειάζεται.

2. Ὑποθέτουμε, γιά νά φθάσουμε σέ ἀντίφαση, ὅτι ὁ ἀλγόριθμος "παράγει" κάθε μετάθεση τοῦ συνόλου μέ πιθανότητα $1/n!$. Γιά κάθε τιμή τοῦ K, ὑπάρχουν n διαφορετικά ἐνδεχόμενα· ἔτσι, ὁ συνολικός ἀριθμός ἐνδεχομένων εἶναι n^n. Προσέξτε ὅτι $n^n > n!$ γιά $n \geq 2$· ἔτσι, ὀφείλουν νά ὑπάρχουν διαφορετι. "συνολικά" ἐνδεχόμενα τά ὁποῖα ἀντιστοιχοῦν στήν ἴδια μετάθεση. Προσέξτε ἀκόμη ὅτι κάθε "συνολικό" ἐνδεχόμενο "παράγει" ὁμοιόμορφα, δηλ., μέ πιθανότητα $1/n^n$. Ἔστω n_π ὁ ἀριθμός "συνολικῶν" ἐνδεχομένων πού ἀντιστοιχοῦν στή μετάθεση π. Πρέπει: $n_\pi \cdot \frac{1}{n^n} = \frac{1}{n!} \Rightarrow n_\pi = \frac{n^n}{n!}$. Συνεπῶς, τό $n!$ διαιρεῖ τό n^n. Αὐτό, ὅμως, δέν ἰσχύει γιά $n \geq 3$: τό $(n-1)$ διαιρεῖ τό $n!$ ἀλλά ὄχι τό n^n (διότι τό n^n ἀφήνει ὑπόλοιπο 1 διαιρούμενο διά τοῦ $n-1$).

3. Τό πρόβλημα εἶναι ἐνδιαφέρον στήν περίπτωση μόνο πού τό $P_3(x)$ ἔχει βαθμό τό πολύ $2n$: ἀλλοιῶς, $P_1(x)P_2(x) \not\equiv P_3(x)$ μέ βεβαιότητα. Ἔστω S ἕνα σύνολο ἀπό $2n+1$ τουλάχιστον σημεῖα· τό σύνολο αὐτό εἶναι σταθερό καί χρησιμοποιεῖται ἀπό τόν ἀλγόριθμο πάνω σέ ὁποιαδήποτε εἴσοδο ($P_1(x)$, $P_2(x)$ καί $P_3(x)$). Ὁ ἀλγόριθμος ἔχει ὡς ἑξῆς:

- Διάλεξε ἕνα σημεῖο $r \in S$ ὁμοιόμορφα καί τυχαῖα.
- Ὑπολόγισε τήν τιμή $p_1(r)\, p_2(r) - p_3(r)$.
- Ἄν $p_1(r)\, p_2(r) - p_3(r) \neq 0$

  τότε ἐπίστρεψε $(\, p_1(x)\, p_2(x) \not\equiv p_3(x)\,)$

  ἀλλοιῶς ἐπίστρεψε $(\, p_1(x) \cdot p_2(x) \equiv p_3(x)$ πιθανόν$)$

Ἀνάλυση σφάλματος:

1. Ἄν $p_1(x)\, p_2(x) \equiv p_3(x)$, τότε $p_1(r)\, p_2(r) = p_3(r)$ γιά κάθε r, ἐπομένως: Πιθανότητα$(\, p_1(r)\, p_2(r) - p_3(r) = 0\,) = 1$ καί ὁ ἀλγόριθμος ὀρθά θά ἀποφασίσει $(p_1(x) \cdot p_2(x) \equiv p_3(x)$ πιθανόν$)$
2. Ἄν $p_1(x)\, p_2(x) \not\equiv p_3(x)$, τότε ὑπάρχει r τέτοιο ὥστε $p_1(r)\, p_2(r) = p_3(r)$, καί τότε ὁ ἀλγόριθμος, γιά τέτοιο r, ἐσφαλμένα ἀποφασίζει $(\, p_1(x) \cdot p_2(x) \equiv p_3(x)$ πιθανόν$)$. Ἀφοῦ, ὅμως, τό πολυώνυμο $p_1(x) \cdot p_2(x) - p_3(x)$ ἔχει βαθμό τό πολύ $2n$, ὑπάρχουν τό πολύ $2n$ τέτοια r στό σύνολο S, καί ἡ πιθανότητα σφάλματος εἶναι $\leq \dfrac{2n}{|S|}$. Ἡ πιθανότητα αὐτή μπορεῖ νά γίνει μικρή εἴτε διαλέγοντας τό $|S|$ νά εἶναι μεγάλο, εἴτε "ἐπαναλαμβάνοντας" τόν ἀλγόριθμο πολλές φορές — μέ k ἐπαναλήψεις, ἡ πιθανότητα σφάλματος εἶναι $\leq \left(\dfrac{2n}{|S|}\right)^k$.

5. Ἄνω φράγμα:

$x_1 \leftarrow x \cdot x$

4. Ὑποθέτουμε, γιά νά φθάσουμε σέ ἀντίφαση, ὅτι μποροῦμε νά λύσουμε στό μοντέλο τοῦ προγράμματος εὐθείας γραμμῆς τό πρόβλημα τοῦ μιγαδικοῦ πολλαπλασιασμοῦ μέ δύο μόνο πολλαπλασιασμούς.

Ἔστω ὅτι ὁ πρῶτος πολλαπλασιασμός εἶναι: $w_1 \leftarrow x_1 \cdot x_2$, ὅπου

$x_1 = \alpha_1 a + \beta_1 b + \gamma_1 c + \delta_1 d$ καί

$x_2 = \alpha_2 a + \beta_2 b + \gamma_2 c + \delta_2 d$, ὅπου τά $\alpha_i, \beta_i, \gamma_i$ καί δ_i εἶναι ἀκέραιοι. Ἔστω ὅτι ὁ δεύτερος πολλαπλασιασμός εἶναι:

$w_2 \leftarrow x_3 \cdot x_4$, ὅπου:

$x_3 = \alpha_3 a + \beta_3 b + \gamma_3 c + \delta_3 d + \kappa_1 w_1$ καί

$x_4 = \alpha_4 a + \beta_4 b + \gamma_4 c + \delta_4 d + \kappa_2 w_2$.

<u>Πρόταση 1</u>: $\kappa_1 = \kappa_2 = 0$

<u>Ἀπόδειξη</u>: Ὑποθέτουμε, γιά νά φθάσουμε σέ ἀντίφαση, ὅτι $\kappa_1 \neq 0$ ἤ $\kappa_2 \neq 0$. Ἔστω, χωρίς βλάβη τῆς γενικότητας, ὅτι $\kappa_1 \neq 0$. Ἀφοῦ ὁ ὅρος w_1 περιέχει μόνο ὅρους βαθμοῦ 2, τό γινόμενο $x_3 \cdot x_4$ θά περιέχει τότε ὅρους βαθμοῦ μεγαλύτερου ἀπό 2. Ἀντίφαση.

<u>Πρόταση 2</u>: Τά w_1 καί w_2 ἔχουν τήν μορφή $(\alpha a + \beta b)(\gamma c + \delta c$

<u>Ἀπόδειξη</u>: Τά w_1 καί w_2 ἔχουν τήν γενική μορφή πού δόθηκε πιό πάνω μέ $\kappa_1 = \kappa_2 = 0$. Οἱ ἔξοδοι τοῦ προγράμματ ὀφείλουν νά εἶναι γραμμικοί συνδυασμοί τῶν w_1 καί w_2, δηλ.,

$$ad + bc = \lambda_1 w_1 + \lambda_2 w_2$$
$$ac - bd = \lambda_3 w_1 + \lambda_4 w_2.$$

Ἔστω A_1 καί A_2 οἱ συντελεστές τοῦ a^2 στά w_1 καί w_2, ἀντίστοιχα. Τότε:

$$\lambda_1 A_1 + \lambda_2 A_2 = 0$$
$$\lambda_3 A_1 + \lambda_4 A_2 = 0$$

Ἂν $A_1 \neq 0$, τότε: $\frac{\lambda_1}{\lambda_2} = \frac{\lambda_3}{\lambda_4} = -\frac{A_2}{A_1}$, τό ὁποῖο συνεπάγεται ὅτι οἱ δύο ἔξοδοι, $ad+bc$ καί $ac-bd$, εἶναι παράλληλες ἡ μία της ἄλλης: πράγματι,

$$ac - bd = -\frac{A_2}{A_1}\lambda_4 w_1 + \lambda_4 w_2$$

$$= \lambda_4\left(-\frac{A_2}{A_1} w_1 + w_2\right)$$

καί $$ad + bc = -\frac{A_2}{A_1}\lambda_2 w_1 + \lambda_2 w_2$$

$$= \lambda_2\left(-\frac{A_2}{A_1} w_1 + w_2\right),$$

ὁπότε: $\frac{ad+bc}{ac-bd} = \frac{\lambda_2}{\lambda_4}$, τό ὁποῖο εἶναι ἀντίφαση. Ἄρα, $A_1 = 0$

Μέ ὅμοιο τρόπο, δείχνουμε ὅτι $A_2 = 0$.
Μέ ὅμοιο τρόπο, δείχνουμε ὅτι οἱ συντελεστές τῶν ὑπολοίπων τετραγώνων (b^2, c^2 καί d^2) στά w_1 καί w_2 εἶναι ἐπίσης 0.
Μέ ὅμοιο τρόπο, δείχνουμε ὅτι οἱ συντελεστές τῶν ὑπολοίπων δευτεροβαθμίων ὅρων πού δέν εἶναι παρόντες στίς ἐξόδους (δηλ., ab καί cd) εἶναι ἐπίσης 0 στά w_1 καί w_2. Αὐτό συμπληρώνει τήν ἀπόδειξη ὅτι τά w_1 καί w_2 ἔχουν τήν ζητούμενη μορφή.

Ἀπό τήν Πρόταση 2, προκύπτει ὅτι:

$$w_1 = h_1 ac + h_2 ad + h_3 bc + h_4 bd$$
$$w_2 = g_1 ac + g_2 ad + g_3 bc + g_4 bd$$

Θυμηθεῖτε ἐπίσης ὅτι:

$$
\begin{aligned}
ad + bc &= \lambda_1 w_1 + \lambda_2 w_2 = \\
&= (\lambda_1 h_1 + \lambda_2 g_1)\, ac + (\lambda_1 h_2 + \lambda_2 g_2)\, ad + \\
&+ (\lambda_1 h_3 + \lambda_2 g_3)\, bc + (\lambda_1 h_4 + \lambda_2 g_4)\, bd
\end{aligned}
$$

$$
\begin{aligned}
ac - bd &= \lambda_3 w_1 + \lambda_4 w_2 \\
&= (\lambda_3 h_1 + \lambda_4 g_1)\, ac + (\lambda_3 h_2 + \lambda_4 g_2)\, ad + \\
&+ (\lambda_3 h_3 + \lambda_4 g_3)\, bc + (\lambda_3 h_4 + \lambda_4 g_4)\, bd
\end{aligned}
$$

Ἐξισώνοντας τούς συντελεστές τῶν ad, bc, ac, bd στά δύο μέλη κάθε μίας ἀπό τίς παραπάνω ἐξισώσεις, παίρνουμε ἕνα σύστημα 8 ἐξισώσεων μέ 8 ἀγνώστους ($h_1, h_2, h_3, h_4, g_1, g_2, g_3$ καί g_4), τό ὁποῖο ἐπιλύεται γιά νά δώσει:

$$h_2 = h_3 = \frac{-\lambda_4}{\lambda_3\lambda_2 - \lambda_4\lambda_1}$$

$$-h_4 = h_1 = \frac{\lambda_2}{\lambda_3\lambda_2 - \lambda_4\lambda_1}$$

$$g_2 = g_3 = \frac{\lambda_3}{\lambda_3\lambda_2 - \lambda_4\lambda_1}$$

$$-g_4 = g_1 = \frac{-\lambda_1}{\lambda_3\lambda_2 - \lambda_4\lambda_1}$$

Ὅμως:

$$w_1 = (\alpha a + \beta b)(\gamma c + \delta d) = \alpha\gamma(ac) + \underline{\alpha\delta}(ad) + \beta\gamma(bc) + \beta\delta(bd)$$

$$\parallel$$

$$h_1\, ac + h_2\, ad + h_3\, bc + h_4\, bd$$

$\therefore\ \alpha\delta = \beta\gamma$ καί $-\beta\delta = \alpha\gamma \Rightarrow (\alpha\delta)(-\beta\delta) = (\beta\gamma)(\alpha\gamma)$

$\Leftrightarrow -\alpha\beta\delta^2 = \alpha\beta\gamma^2 \underset{\alpha\beta\neq 0}{\Longleftrightarrow} -\delta^2 = \gamma^2 \Rightarrow \gamma = \delta = 0$, ἀντίφασ.