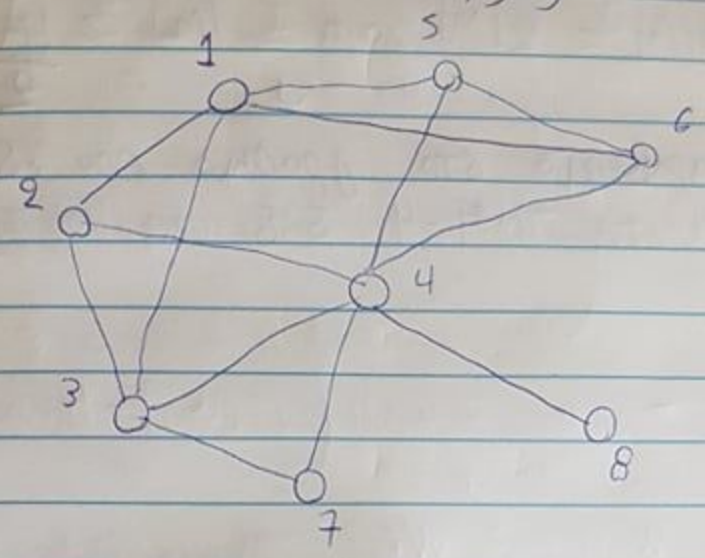
Ασκηση 1 Μπάρδας Γιάννης 2765



α) Ο αλγοριθμος επιλεγει τις ακμες 1-3, 2-4, 5-6 αφα το ταιριασμα M το οποιο δεν ειναι μεγιστο ειναι το $M = \{1-3, 2-4, 5-6\}$

ενω ενα τελειο ταιριασμα ειναι το $M^* = \{1-2, 5-6, 3-7, 4-8\}$

β) Εστω A το συνολο των κορυφων που επιλεξε ο αλγοριθμος (στο τελος δεν ειναι ελευθεροι) το ταιριασμα M αποτελειται απο ακμες απο τους κορυφους του A. Αρα αφου χρειαζονται 2 κορυφοι ανα ακμη.

εχουμε $M = \frac{A}{2} \Rightarrow A = 2M$

Επισης καθε ακμη του M^* καλυπτεται απο

τουλαχιστον 1 κομβο του A οπα

$$|M^*| \leq |A| = 2|M| \text{ οπ. } |M| \geq \frac{|M^*|}{2}$$

Επίσης στο παραδειγμα στο γραφημα που εδωσαν εχουμε $|M| = 3$ ενω $|M^*| = 4$ δλδ ισχυει $|M| \geq \frac{|M^*|}{2}$

Ασκηση 2

Ο γενικευμενος απληστος αλγοριθμος για ανθαιρετα βαση ειναι ο:

Αρχικοποιηση $U \leftarrow X$, $C \leftarrow \emptyset$

Ενοσω $U \neq \emptyset$

επιλεγουμε $S \in F$ που ελαχιστοποιει
η με ελαχιστη τιμη

$$\frac{w_i}{|S_i - \{S_1 \cup \dots \cup S_{i-1}\}|}$$

$$U \leftarrow U - S, \quad C \leftarrow C \cup \{S\}$$

Ο απληστος αλγοριθμος ειναι $\rho(n)$ - προσεγγιστικος με $\rho(n) = H(\max\{|S| : S \in F\}) = H(d)$, $H(d) = \sum_{i=1}^{d} \frac{1}{i}$ και $n = |X|$

Εστω S_i το i-οστο σύνολο που επιλέγει ο αλγόριθμος η προσθήκη του S_i έχει κόστος w_i αφού αυξάνει το $|C|$ κατα w_i μονάδες. $S_i - \{S_1 \cup \dots \cup S_{i-1}\}$ είναι τα στοιχεία του S_i που καλύπτονται για πρώτη φορά.

Κόστος ανα νέο στοιχείο $c_x = \dfrac{w_i}{|S_i - \{S_1 \cup \dots \cup S_{i-1}\}|}$

$|C| = \sum_{x \in A} c_x$ Αποδείξουμε στο βέλτιστο κάλυμμα

κόστος $\sum_{S \in C^*} \sum_{x \in S} c_x \geq \sum_{x \in A} c_x = |C|$

$w_{i-1} - w_i$ = στοιχεία που καλύπτονται για πρώτη φορά από το S_i Εχουμε

$$\sum_{x \in S} c_x = \sum_{i=1}^{k} (w_{i-1} - w_i) \frac{w_i}{|S_i - \{S_1 \cup \dots \cup S_{i-1}\}|} \leq$$

$$\leq \sum_{i=1}^{k} (w_{i-1} - w_i) \cdot \frac{w_i}{|S - \{S_1 \cup \dots \cup S_{i-1}\}|} =$$

$$= \sum_{i=1}^{k} \left(\frac{w_{i-1} - w_i}{w_{i-1}} \cdot w_i \right) =$$

$$= \sum_{i=1}^{k} w_i \sum_{j=w_i+1}^{w_{i-1}} \frac{1}{w_{i-1}} \leq \sum_{i=1}^{k} w_i \sum_{j=w_i+1}^{w_{i-1}} \frac{1}{j}$$

Επομένως

$$\sum_{x\in S} c_x \leq \sum_{i=1}^{k} w_i \left(\sum_{j=1}^{u_{i-1}} \frac{1}{j} - \sum_{j=1}^{u_i} \frac{1}{j} \right)$$

$$= \sum_{i=1}^{k} w_i \left(H(u_{i-1}) - H(u_i) \right) =$$

~~= wall (H(ui-1)) - H(ui~~ $= w_{all} \left(H(u_0) - H(u_k) \right) =$

$= w_{all} \cdot H(|S|)$, $w_{all} = \sum_{i=1}^{k} w_i$ άρα ισχύει

$$\sum_{x\in S} c_x \leq w_{all} H(|S|)$$

άρα

$$\leq w_{all} H(d)$$

για d μέγιστο μέγεθος απόδοσης S_i

Ασκηση 3

α) Ο νόμος το πρόβλημα αποτελεί γενίκευση του κομβικού καλύμματος αν θεωρήσουμε

Γράφημα $G = (V, E)$ με $V = |A| = \{a_1, a_2, \ldots a_k\}$ και $E = M = \{M_1, M_2, \ldots, M_k\}$ όπου $\forall M_i$ είναι το σύνολο όλων των δυνατών ακμών από τους κόμβους (τιμές a_i) που περιέχονται στο B_i.

(5)

Σημαδη το $Bi = \{a_1, a_2, a_3\}$ αν $Mi = \{a_1-a_2, a_2-a_3, a_1-a_3\}$ (ακμες)
και $\forall Mi, Bi \neq \emptyset$, $\forall Mi \subseteq E$

Αν εφαρμοσουμε τον αλγοριθμο κορυφικου καλυμματος σε αυτο το γραφημα G το συνολο των κορυφων με το A και το συνολο των ακμων με το B μεσω του M τοτε μπορουμε ευκολα να διαπιστωσουμε οτι το συνολο του κορυφικου καλυμματος ισουται με το συνολο κορυφων H. Οντως αν παρουμε την τομη του H με οποιοδηποτε $Bi \neq \emptyset$ που περιεχει τις κορυφες των ακμων του συνολου Mi τοτε καθε στοιχειο του συνολου κορυφων H (κορυφικο καλυμμα) περιεχεται σε τουλαχιστον 1 Bi και δεν μπορει να υπαρχει κανενα Bi που να μην εχει εστω 1 κορυφο (κορυφη) απο το συνολο (κορυφικου καλυμματος) H.

β) Αφου δειξαμε οτι το προβλημα ευρεσης συνολου κορυφων H ειναι ισοδυναμο με το προβλημα ευρεσης κορυφικου καλυμματος για το γραφημα G που ορισαμε στο ερωτημα α μπορουμε να ορισουμε το ~~προβλημα~~

τοτε ~~Ακέραιο πρόβλημα~~

Ακέραιο προγραμμα

$$\forall i \in A(\text{η } V) \quad x_i = \begin{cases} 1, & \text{αν } a_i \in H \ (=) \ a_i \in \text{κ(αντιμα} \\ & \text{και } x_i + x_j \geq 1, (i,j) \in E \\ & \in M \\ 0 & \text{αν } a_i \notin H \ \text{δηλ } a_i \notin \text{κ} \end{cases}$$

Ακέραιο Μαθημα

$$\min \sum c_i x_i \quad , x_i + x_j \geq 1 \quad (i,j) \in E \ (\text{η } M)$$

$$x_i \in \{0,1\} \ , i \in A(\text{η } V)$$

γ) Το Γραμμικο προγραμμα

$$\min \sum c_i x_i \qquad x_i + x_j \geq \frac{1}{6} \quad (i,j) \in E \ (\text{μ}$$

τ.ω. $a_i, a_j \in B_i$

$$0 \leq x_i \leq 1 \qquad i \in V \ \text{η} \ (A)$$

$$\forall B_j \in B \quad \sum_{a_j \in B_j} x_j \geq 6$$

το ίδιο συνολο στο 6

Αφου το προβλημα κορυφης ειναι ισοδυναμο με το προβλημα κοβικων καλυμματος για το γραφημα G τοτε (α) εχουμε

το προσεγγιστικό βελτιστης κανονης

$H = \phi$

Υπολογίζουμε βελτιστη λυση x' για το γραμμικο προβλημα

Για καθε $u \in A$

αν $x'(u) \geq 1/b$

$H = H \cup \{v\}$

επιστροφη H

Εστω H^* η βελτιστη ~~λυση~~ κανονη με βαρος $w(H^*)$ και εστω $x_1', \dots, x_n'$ μια βελτιστη λυση του γραμμικου προβληματος με βαρος $W_{LP} = \sum_{i \in A} c_i x_i$

~~W(H)~~ τοτε $W_{LP} \leq w(H^*)$

$\forall$ ακμη $\{i,j\} \in E(M)$ $x_i' + x_j' \geq \frac{2}{b}$

$\max\{x_i, x_j\} \geq 1/b$

Επιπλεον $W_{LP} = \sum_{i \in A} c_i x_i \geq$

$\geq \sum_{i \in H} c_i x_i \geq \frac{1}{b} \sum_{i \in H} c_i = \frac{1}{b} w(H)$

αρα $W(P) \geq \frac{1}{b} W(H)$

Επισης εχουμε $W(P) \leq W(H^*) \Rightarrow b\,W(P) \leq b\,W(H^*)$

αρα $W(H) \leq b\,W(P) \leq b\,W(H^*)$

b προσεγγιστικος

Ο αλγοριθμος παραγει μια λυση με βαρος το πολυ b - πλασιο απο το ελαχιστο δυνατο.

Ασκηση 4

α)

i) Αφου a, b αρτιοι $\Rightarrow a \bmod 2 = 0$, $b \bmod 2 = 0$ και $a/2 = a \operatorname{div} 2$ και $b/2 = b \operatorname{div} 2$

αρα το gcd μπορει να γραφτει

$$\gcd\left(2 \cdot (a/2),\ 2 \cdot (b/2)\right) =$$

οπως ισχυει $\gcd(na, nb) = n \gcd(a, b)$ αρα

$$= 2 \gcd(a/2,\ b/2)$$

ii)

ii) Για να αποδείξω ότι

$$\gcd(a,b) = \gcd(a, b/2)$$

Αρκεί 1. Να Αν $k|a$ και $k|b$ τότε $k|a$ και $k|b/2$
2. Να Αν $k|a$ και $k|b/2$ τότε $k|a$ και $k|b$

Αυτό θα δείξει ότι το σύνολο των διαιρετών των (a,b) και $(a,b/2)$ είναι ίδια.

Πρώτα για το 1:

Έχουμε a περιττό, b οτιδ
Χρειάζεται να δείξουμε μόνο ότι k διαιρεί $b/2$

Άρα $b^* = \frac{b}{2} \iff b = 2b^*$

Επειδή k διαιρεί το a και το a περιττός τότε και το k είναι περιττός
και αφού διαιρεί το b, $k|b \iff k|2b^*$
το 2 και το k είναι αμοιβαία πρώτοι και
άρα το $\gcd(k,2) = 1$
και αλλιώς ισχύει ότι $x|yz$ και $\gcd(x,y)=1$ τότε $x|z$

Και άρα το αφού
$k|2b^*$ και $\gcd(k,2) = 1$ τότε

$k|b^* \iff k|b/2$

2. Για το 2 έχουμε

(10)

Στο 2 πρεπει νδο k διαιρει b, k|b
2.(Αν k|a και k|b/2 τοτε k|b και k|a)
Εχουμε αφου το k διαιρει το b/2 (k|b/2)

αρα $\frac{b}{2} = kq$ για καποιο q ακεραιο

επομενως $b = k(2q)$ αρα το k διαιρει και το b.

πριν αποδειξαμε τα 1,2 τωρα δειξαμε
οτι τα συνολα διαιρετων των (a,b) και (a,b/2)
ειναι ιδια και αρα ειναι ιδια και τα μεγιστα στοιχεια
τους.

iii) Τα a,b περιττοι (a-b) αρτιος

Εστω $d = gcd(a,b)$ αρα $d|a$ και $d|b$

οπου το d ειναι περιττος αφου τα a,b ειναι περιττοι. (αν ενδειξη)

Ισοδυναμα το $d|(a-b)$ και $d|b$

a-b αρτιος

αρα $d|a-b$ (=) $d|2\cdot(|a-b|)/2$ (=)

(=) αφου $d|2\cdot(a-b)/2$ και
το k, 2 αριθμοι πρωτοι $gcd(k,2)=1$

αρα $k|(a-b)/2$ αρα $k|(a-b)/2$ και
$k|b$

άρα $k \mid b$ και $k \mid (a-b)/2$ τότε
τα σύνολα (a, b) και $((a-b)/2, b)$ έχουν ίδια
σύνολα και άρα ίδιο μέγιστο στοιχείο.

β) $g = 1$ (μεταβλητή για τον υπολογισμό του gcd.

Όσο (mod2(a) == 0 ΚΑΙ mod2(b) == 0)
    a = div2(a)
    b = div2(b) (right shift)
    g = 2 * g (left shift) (div ½(g))

→ Όταν ένα ή και οι 2 περιττοί

Όσο b > 0

    Αν (mod2(b) == 0) ← b άρτιο
        b = div2(b)

    Αν (mod2(a) == 0) ← a άρτιο a

        a = div2(a)

    ← κανένα άρτιο
    Αν (mod2(a) == 1 ΚΑΙ mod2(b) == 1)

        ~~[illegible]~~
        t = div2(|a - b|)
        If (b < a) → a = t
        αλλιώς b = t

Επέστρεψε a·g

Ασκηση 5

α)

Για $C_1 = M^{e_1} \bmod n_1$, $C_2 = M^{e_2} \bmod n_2$, $C_3 = M^{e_3} \bmod n_3$

εχουμε $\gcd(n_1, n_2) \neq 1$ Αυτο σημαινει οτι υπαρχει ακεραιος K που διαιρει ακριβως και τον n_1 και τον n_2 $K | n_1$ και $K | n_2$ Αυτο σημαινει οτι το ευρος των συνδιαφων των πρωτων $p_1 - q_1$ και των συνδιαφων των πρωτων $p_2 - q_2$ ~~βρισκεται στο συνολο των πρωτων μεσα στο διαστημα [1, gcd(n1, n2)]~~ μπορει να περιοριστει και να ελενξουμε μονο τους συνδιαφους ~~αριθμους~~ πρωτων στο διαστημα $[1, \gcd(n_1, n_2)]$ Επισης αν η παραγοντοποιηση γινει για το μικροτερο των n_1, n_2 τοτε θα μειωθουν οι εγκυροι συνδιαφοι πρωτων p, q απο το διαστημα $[1, \gcd(n_1, n_2)]$

β) Εχουμε $\gcd(n_1, n_2) = \gcd(n_2, n_3) = \gcd(n_3, n_1) = 1$ αρα ολοι πρωτοι μεταξυ τους.

Απο κινεζικο θεωρημα για $C_1 = M^3 \bmod n_1$, $C_2 = M^3 \bmod n_2$ $C_3 = M^3 \bmod n_3$ (αφου $e_1 = e_2 = e_3 = 3$) εχουμε το συστημα για $a = M^3$

$$X \equiv M^3 \bmod n_1 = C_1$$
$$X \equiv M^3 \bmod n_2 = C_2$$
$$X \equiv M^3 \bmod n_3 = C_3$$
$$X \equiv M^3 \bmod n \quad \text{για } n = n_1 n_2 n_3$$

Η ενα προσπαθει να το λυσει να βρει το X