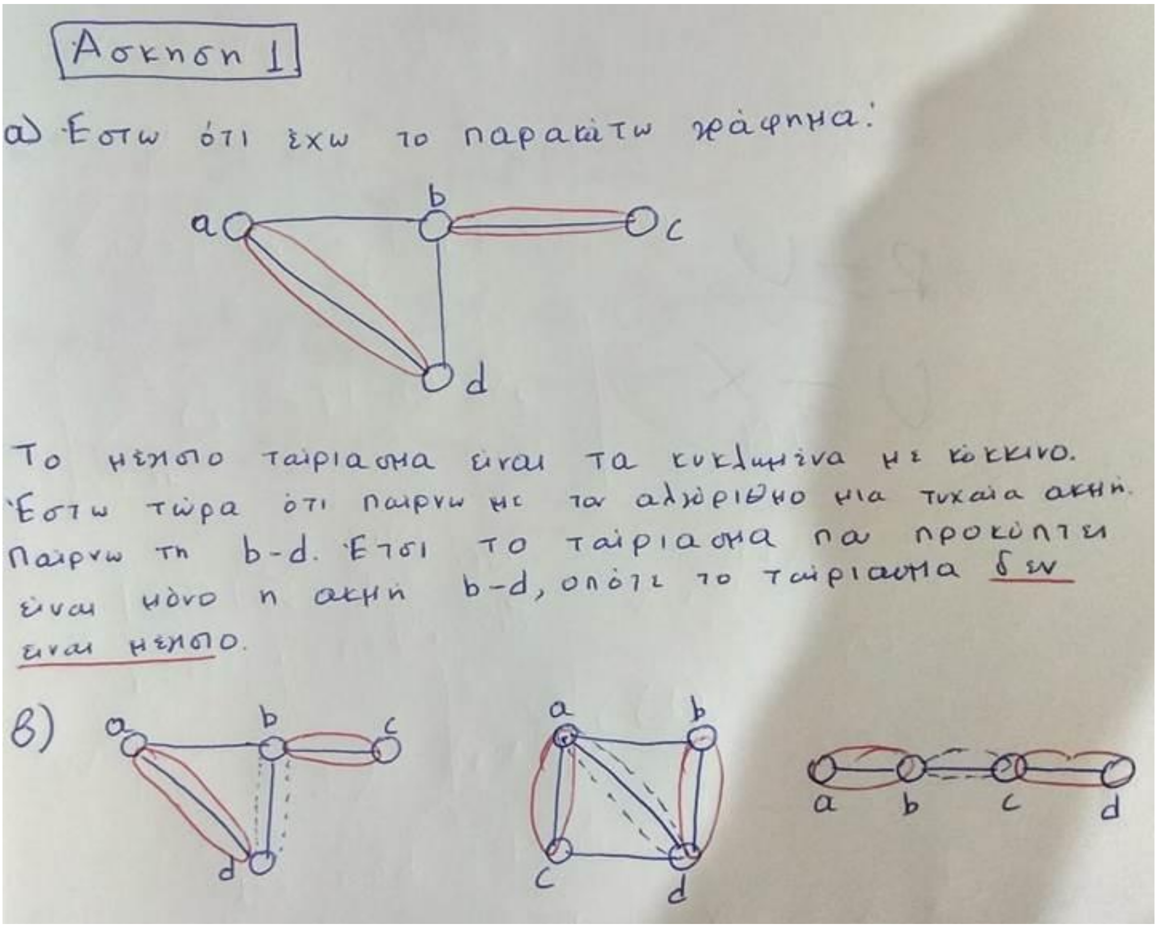
Γεώργιος Δημόπουλος

Α.Μ. 2964

Άσκηση 1 (Υπολογισμός ταιριάσματος με τοπική αναζήτηση)


Ασκηση 1

α) Έστω ότι έχω το παρακάτω γράφημα:

Το μέγιστο ταίριασμα είναι τα κυκλωμένα με κόκκινο. Έστω τώρα ότι παίρνω με τον αλγόριθμο μια τυχαία ακμή. Παίρνω τη b-d. Έτσι το ταίριασμα πα προκύπτει είναι μόνο η ακμή b-d, οπότε το ταίριασμα δεν είναι μέγιστο.

β)

Για το β ερώτημα παρατηρώ, ότι αν επιλέξω μια τυχαία ακμή που δεν είναι ακμή του μέγιστου ταιριάσματος, τότε αυτή η τυχαία ακμή που επιλέγω, οι κόμβοι της είναι σίγουρα τα άκρα των ακμών που ανήκουν στο μέγιστο ταίριασμα. Συνεπώς αν πάρω μια τυχαία ακμή που δεν ανήκει στο μέγιστο ταίριασμα θα ακυρώσει τις άλλες δύο ακμές του μέγιστου ταιριάσματος, οπότε το πλήθος των ακμών του ταιριάσματος θα υποδιπλασιαστεί.

Άσκηση 2 (Κάλυψη συνόλου με βάρη)

Άσκηση 2

Παραλλαγή του αλγορίθμου:

$X =$ σύνολο αντικειμένων

$F =$ οικογένεια υποσυνόλων του X, $X = \bigcup_{S \in F} S$

Το σύνολο $C \subseteq F$ καλύπτει το X αν $\bigcup_{S \in C} = X$

Άπληστος αλγόριθμος:

1. αρχικοποίηση: $U \leftarrow X$, $C \leftarrow \emptyset$
2. Ενόσω $U \neq \emptyset$
3. επιλέγουμε $S \in F$ που ελαχιστοποιεί το κλάσμα $\frac{w_i}{|S_i \cap U|}$
4. $U \leftarrow U - S$, $C \leftarrow C \cup \{S\}$

Ορίζω ως $c_x = w_i / |S_i \cap U|$ για όλα τα $x \in S_i \cap U$

$\sum_{S_i \in C} w_i = \sum_{x \in U} c_x$. Επίσης $H(d) = \sum_{i=1}^{d} \frac{1}{i}$

Για κάθε σύνολο S_k, το $\sum_{x \in S_k} c_x = H(d) \cdot w_k$

Έστω C^* συμβολίζει τη βέλτιστη κάλυψη συνόλων.

$$w_i \geq \frac{1}{H(d^*)} \sum_{x \in S_i} c_x$$

$$\sum_{S_i \in C^*} \sum_{x \in S_i} c_x \geq \sum_{x \in X} c_x$$

$$w^* = \sum_{S_i \in C^*} w_i \geq \sum_{S_i \in C^*} \frac{1}{H(d^*)} \sum_{x \in S_i} c_s \geq \frac{1}{H(d^*)} \sum_{x \in X} c_x = \frac{1}{H(d^*)} \sum_{S_i \in C} w_i$$

Άρα $w^* \geq \frac{1}{H(d^*)} \cdot \sum_{S_i \in C} w_i \Rightarrow w^* H(d^*) \geq C(I) \Rightarrow$

$$C(I) \leq w^* H(d^*) \Rightarrow \boxed{\frac{C(I)}{C^*(I)} \leq H(d^*)}$$

Άσκηση 4 (Δυαδικός αλγόριθμος υπολογισμού του μέγιστου κοινού διαιρέτη)

Άσκηση 4

α) 1) Αν a,b άρτιοι τότε

$a=2\kappa$ $\quad$ $\beta=2\lambda$

με $\kappa=\frac{a}{2}$ $\quad$ με $\lambda=\frac{\beta}{2}$

Τότε $gcd(a,\beta)=gcd(2\kappa,2\lambda)=2gcd(\kappa,\lambda)=2gcd(\frac{a}{2},\frac{\beta}{2})$

2) a περιττος $\quad$ β αρτιος

$a=2\kappa+1$ $\quad$ $\beta=2\lambda$

Επειδή a περιττός, έχουμε ότι $a \bmod 2 \neq 0$

Αφού το 2 δω διαιρεί τον a εχω:

$gcd(a,\beta)=gcd(a,2\frac{\beta}{2})=gcd(a,\frac{\beta}{2})$

3) a περιττος $\quad$ β περιττος

$a=2\kappa+1$ $\quad$ $\beta=2\lambda+1$

Εστω $d=gcd(a,\beta)$

Τότε $d=a\cdot p+\beta q$, με $p,q\in Z$

$d=a\cdot p+\beta\cdot q \Rightarrow d=a\cdot p-\beta p+\beta\cdot p+\beta q \Rightarrow$

$d=(2\kappa+1)p-(2\lambda+1)p+\beta(p+q) \Rightarrow d=(2\kappa-2\lambda)p+b(p+q) \Rightarrow$

$d=(\kappa-\lambda)\cdot p+\beta(p+q) \Rightarrow gcd(a,\beta)=gcd(\frac{a-\beta}{2},\beta)$

Αυτό που κάνω τώρα είναι να ελέγχω κάθε φορά αν είναι περιττοί ή άρτιοι οι αριθμοί και αναλόγως να ακολουθήσω την κάθε περίπτωση. Έπειτα κάνω το ίδιο μέχρι ένα από τα α,β=1 ή ένα από τα α,β=0. Επειδή ξέρω ότι gcd(k,1)=1 και ότι gcd(k,0)=k. Τώρα το θέμα μου είναι να δω πότε θα σταματήσει ο αλγόριθμος. Σε κάθε βήμα υποδιπλασιάζεται ένας από τους α,β. Ξέρω ότι α>=β. Οπότε θα σταματήσω, όταν $\alpha/2^\kappa=1$. Δηλαδή όταν $\alpha=2^\kappa$ => $\log_2(\alpha)=\log_2(2^\kappa)$ => $\kappa=\log_2(\alpha)$. Έτσι ο αλγόριθμος μας θα χρειαστεί χρόνο **$O(\log_2(\alpha))$**.

Άσκηση 5 (RSA)

Άσκηση 5

α) Επειδή το $gcd(n_1, n_2) \neq 1$, ξέρω ότι τα n_1, n_2 έχουν ένα κοινό παράγοντα 7/2

Έστω ότι $n_1 = K \cdot L$

$C_1 = M^{e_1} \bmod n_1 \Rightarrow M = C_1^{d_1} \bmod n_1$

Δεν ξέρω μόνο το d_1. Το $\boxed{d_1}$ όμως είναι το πολλαπλασιαστικό αντίστροφο του $\boxed{e_1 \bmod (K-1)(L-1)}$

β) $x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

⋮

$x \equiv a_n \pmod{m_n}$

$m = m_1 \cdot m_2 \cdots m_n$

✓ $\forall i \in \{1, 2, \ldots, n\}$, $M_i := \frac{m}{m_i}$

✓ $gcd(M_i, m_i) = 1$

✓ $\overline{M_i}$: Το πολλαπλασιαστικό αντίστροφο του $M_i \pmod{m_i}$

Η τιμή $\boxed{b = a_1 M_1 \overline{M_1} + \ldots + a_n M_n \overline{M_n}}$ είναι ταυτόχρονη λύση για όλες τις γραμμικές ισοτιμίες

$C_1 = M^3 \bmod n_1 \Rightarrow \boxed{M} = C_1^{d_1} \bmod n_1$, με $a_1 = C_1^{d_1}$

$C_2 = M^3 \bmod n_2 \Rightarrow \boxed{M} = C_2^{d_2} \bmod n_2$, με $a_2 = C_2^{d_2}$

$C_3 = M^3 \bmod n_3 \Rightarrow \boxed{M} = C_3^{d_3} \bmod n_3$, με $a_3 = C_3^{d_3}$

Από κινέζικο υπόλοιπο έχουμε ότι:

$$\boxed{M = a_1 M_1 \overline{M_1} + a_2 M_2 \overline{M_2} + a_3 M_3 \overline{M_3}}$$