Πανεπιστήμιο Ιωαννίνων – Τμήμα Μηχανικών Η/Υ και Πληροφορικής
Προηγμένη Σχεδίαση Αλγορίθμων και Δομών Δεδομένων [MYE028]
Εαρινό Εξάμηνο 2020

4ο σύνολο ασκήσεων. Ημερομηνία παράδοσης: Πέμπτη 18/6/2020
Παράδοση εργασιών μέσω eCourse

Άσκηση 1 (Υπολογισμός ταιριάσματος με τοπική αναζήτηση)

Έστω $G = (V, E)$ ένα απλό γράφημα. Ένα σύνολο ακμών $M \subseteq E$ του G αποτελεί ένα *ταίριασμα* αν στο υπογράφημα $G_M = (V, M)$ του G κάθε κορυφή έχει βαθμό ίσο με 0 ή 1. (Δηλαδή κάθε κορυφή $v \in V$ έχει το πολύ ένα γείτονα στο G_M.) Το ταίριασμα M είναι *μέγιστο* αν για κάθε άλλο ταίριασμα M' του G ισχύει $|M| \geq |M'|$.

Όπως έχουμε δει στο μάθημα, ο υπολογισμός ενός μέγιστου ταιριάσματος μπορεί να γίνει σε πολυωνυμικό χρόνο, αλλά οι αλγόριθμοι που το επιτυγχάνουν αυτό σε γενικά γραφήματα είναι αρκετά περίπλοκοι. Εδώ θα μελετήσουμε την απόδοση του ακόλουθου απλοϊκού αλγόριθμου:

```
M = ∅;                                   // το ταίριασμά μας είναι αρχικά κενό
for (e = {x, y} ∈ E) {                   // για κάθε ακμή του γραφήματος
    if ( οι κορυφές x και y είναι ελεύθερες)   // έλεγχος αν το M ∪ e είναι ταίριασμα
        M = M ∪ e;
}
```

α. Δώστε ένα παράδειγμα όπου ο παραπάνω αλγόριθμος υπολογίζει ένα ταίριασμα M το οποίο δεν είναι μέγιστο.

β. Δείξτε ότι ο παραπάνω αλγόριθμος υπολογίζει πάντα ένα ταίριασμα M το όποιο έχει μέγεθος $|M| \geq |M^*|/2$, όπου M^* ένα μέγιστο ταίριασμα του G.

Άσκηση 2 (Κάλυψη συνόλου με βάρη)

Μελετάμε την παραλλαγή του προβλήματος της Κάλυψης Συνόλου όταν τα υποσύνολα μας έχουν κάποιο θετικό βάρος. Συγκεκριμένα, μας δίνεται ένα σύνολο με n αντικείμενα $X = \{x_1, x_2, \ldots, x_n\}$, καθώς και μια οικογένεια $\mathcal{F} = \{S_1, S_2, \ldots, S_k\}$ υποσυνόλων του X, όπου η ένωση τους καλύπτει το X. Δηλαδή, $S_i \subseteq X$ για κάθε $S_i \in \mathcal{F}$, και $\bigcup_{i=1}^{k} S_i = X$. Επιπλέον, κάθε σύνολο $S_i \in \mathcal{F}$ έχει ένα θετικό βάρος $w_i > 0$. Μια οικογένεια $\mathcal{C} \subseteq \mathcal{F}$ καλύπτει το X αν $\bigcup_{S_i \in \mathcal{C}} S_i = X$. Το βάρος της οικογένειας $\mathcal{C}$ ισούται με το άθροισμα των βαρών των υποσυνόλων που περιέχονται στη $\mathcal{C}$, δηλαδή $w(\mathcal{C}) = \sum_{S_i \in \mathcal{C}} w_i$. Ο σκοπός μας είναι να υπολογίσουμε μια οικογένεια $\mathcal{C}$ που καλύπτει το X και έχει το ελάχιστο δυνατό βάρος.

Στο μάθημα είχαμε αναλύσει ένα άπληστο αλγόριθμο για την περίπτωση όπου όλα τα σύνολα $S_i \in \mathcal{F}$ έχουν βάρος $w_i = 1$. Προτείνετε μια φυσική γενίκευση αυτού του άπληστου αλγόριθμου για αυθαίρετα βάρη $w_i > 0$ και αποδείξτε ότι επιτυγχάνει λόγο προσέγγισης $H(d)$, όπου d το μέγιστο μέγεθος οποιουδήποτε συνόλου S_i.

Άσκηση 3 (Σύνολο κρούσης μέσω γραμμικού προγραμματισμού)

Μας δίνεται ένα σύνολο με n αντικείμενα $A = \{a_1, a_2, \ldots, a_n\}$, καθώς και μια οικογένεια $\mathcal{B} = \{B_1, B_2, \ldots, B_k\}$ υποσυνόλων του A. Κάθε αντικείμενο $a_i \in A$ έχει ένα θετικό κόστος $c_i > 0$. Λέμε ότι ένα υποσύνολο $H \subseteq A$ αποτελεί ένα *σύνολο κρούσης* της $\mathcal{B}$ αν για κάθε $B_i \in \mathcal{B}$, η τομή $B_i \cap H$ δεν είναι κενή, δηλαδή το H περιέχει τουλάχιστον ένα στοιχείο από κάθε υποσύνολο B_i της οικογένειας $\mathcal{B}$. Το κόστος του H ορίζεται ως το άθροισμα του κόστους κάθε στοιχείου του, δηλαδή $c(H) = \sum_{a_i \in H} c_i$. Στο πρόβλημα του *Συνόλου Κρούσης* θέλουμε να υπολογίσουμε ένα σύνολο κρούσης ελάχιστου κόστους για την οικογένεια $\mathcal{B}$.

α. Δείξτε ότι το παραπάνω πρόβλημα αποτελεί γενίκευση του Κομβικού Καλύμματος.

β. Περιγράψτε ένα Ακέραιο Πρόγραμμα, το οποίο περιγράφει τη βέλτιστη λύση του Συνόλου Κρούσης. *Υπόδειξη: Ορίστε μια μεταβλητή $x_i \in \{0,1\}$ για κάθε αντικείμενο $a_i \in A$.*

γ. Έστω ότι κάθε σύνολο $B_i \in \mathcal{B}$ έχει μέγεθος $|B_i| \leq b$. Περιγράψτε πως μπορούμε να υπολογίσουμε μια b-προσεγγιστική λύση του Συνόλου Κρούσης, μέσω της τεχνικής της χαλάρωσης του Ακέραιου Προγράμματος του ερωτήματος 3β σε Γραμμικό Πρόγραμμα. *Υπόδειξη: Θεωρήστε τη λύση $H = \{a_i \in A : x_i \geq 1/b\}$ η οποία περιέχει τα αντικείμενα a_i για τα οποία $x_i \geq 1/b$.*

Άσκηση 4 (Δυαδικός αλγόριθμος υπολογισμού μέγιστου κοινού διαιρέτη)

Επιθυμούμε να σχεδιάσουμε ένα αλγόριθμο υπολογισμού του μέγιστου κοινού διαιρέτη $gcd(a, b)$ δυο αριθμών a και b που δίνονται μέσω των δυαδικών τους αναπαραστάσεων. Θέλουμε να χρησιμοποιήσουμε μόνο τη διμελή πράξη αφαίρεσης $(x - y)$, και τις μονομελείς πράξεις ελέγχου αρτιότητας, $\boldsymbol{mod2}(x)$, (επιστρέφει το τελευταίο bit της δυαδικής αναπαράστασης του x) και πηλίκου ακέραιας διαίρεσης διά του 2, $\boldsymbol{div2}(x) = \lfloor x/2 \rfloor$, (ισοδυναμεί με κύλιση-δεξιά της δυαδικής αναπαράστασης του x). Έτσι, αποφεύγουμε τις (ενδεχομένως) πιο ακριβές γενικές αριθμητικές πράξεις $x \boldsymbol{mod} y$ και $x \boldsymbol{div} y$, στις οποίες βασίζεται ο αλγόριθμος του Ευκλείδη.

α. Έστω ακέραιοι αριθμοί $a \geq b \geq 0$. Να δειχθεί ότι:
1. Αν οι a και b είναι άρτιοι, τότε ισχύει ότι $gcd(a, b) = 2 \cdot gcd(a/2, b/2)$.
2. Αν ο a είναι περιττός και ο b είναι άρτιος, τότε ισχύει ότι $gcd(a, b) = gcd(a, b/2)$.
3. Αν οι a και b είναι περιττοί, τότε ισχύει ότι $gcd(a, b) = gcd((a - b)/2, b)$.

β. Εκμεταλλευόμενοι το (α), να σχεδιάσετε έναν αποδοτικό αλγόριθμο $BinaryGCD(a, b)$ που υπολογίζει το $gcd(a, b)$ αξιοποιώντας τις πράξεις $x - y$, $\boldsymbol{mod2}(x)$ και $\boldsymbol{div2}(x)$, σε χρόνο $O(\log(a))$, θεωρώντας ότι πράγματι οι πράξεις αυτές επί (δυαδικών αναπαραστάσεων) φυσικών αριθμών x και y απαιτούν μια χρονική μονάδα για την εκτέλεσή τους.

Άσκηση 5 (RSA)

Στην άσκηση αυτή θα διαπιστώσουμε γιατί σε μια υλοποίηση του RSA είναι κακή ιδέα να επιλέξουμε μια μικρή τιμή για τον ιδιωτικό εκθέτη e. Συγκεκριμένα, θα εξετάσουμε την περίπτωση $e = 3$.

Ας υποθέσουμε ότι η Αλίκη στέλνει το ίδιο μήνυμα M σε τρεις φίλους της, χρησιμοποιώντας τα δημόσια κλειδιά τους (e_1, n_1), (e_2, n_2) και (e_3, n_3), όπου $e_1 = e_2 = e_3 = e = 3$. (Προσέξτε ότι ισχύει $M < n_i$ για $i = 1,2,3$.)

Η Εύα υποκλέπτει τα κρυπτογραφημένα μηνύματα $C_1 = M^{e_1} \bmod n_1$, $C_2 = M^{e_2} \bmod n_2$ και $C_3 = M^{e_3} \bmod n_3$, με σκοπό να υπολογίσει το αρχικό μήνυμα M της Αλίκης.

α. Έστω ότι οι ακέραιοι n_1 και n_2 δεν είναι αμοιβαία πρώτοι, δηλαδή $gcd(n_1, n_2) \neq 1$. Περιγράψτε πως μπορεί η Εύα να υπολογίσει το M, παραγοντοποιώντας ένα από τα n_1 και n_2.

β. Υποθέτουμε τώρα ότι οι ακέραιοι n_i είναι μεταξύ τους αμοιβαία πρώτοι, δηλαδή $gcd(n_1, n_2) = gcd(n_2, n_3) = gcd(n_1, n_3) = 1$. Περιγράψτε πως μπορεί η Εύα να υπολογίσει το M, χρησιμοποιώντας το Κινέζικο Θεώρημα Υπολοίπου.

Υπόδειξη: Η υπόθεση $e = 3$ μας είναι χρήσιμη μόνο στην περίπτωση β.