Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Προηγμένα Θέματα Αλγορίθμων

Αλγόριθμοι Δικτύων και Πολυπλοκότητα

Εαρινό εξάμηνο 2021-2022

(ΕΜΠ – ΑΛΜΑ)

Διδάσκοντες: Α. Παγουρτζής – Δ. Φωτάκης – Θ. Λιανέας

2η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 30/6/2022

Άσκηση 1 (Sparsification). (α) Έστω $\boldsymbol{a}, \boldsymbol{x} \in [0,1]^n$, με $\sum_i x_i = 1$ (θα λέμε ότι το $\boldsymbol{x}$ είναι ένα διάνυσμα πιθανοτήτων στο $[n] \equiv \{1,\dots,n\}$). Έστω ακόμη $k(\varepsilon) = \lceil \ln(2)/(2\varepsilon^2) \rceil + 1$. Να δείξετε ότι για κάθε $\varepsilon > 0$, υπάρχει ένα $k(\varepsilon)$-ομοιόμορφο διάνυσμα πιθανοτήτων $\boldsymbol{y}$ στο $[n]$ τέτοιο ώστε $|\boldsymbol{a} \cdot \boldsymbol{x} - \boldsymbol{a} \cdot \boldsymbol{y}| \le \varepsilon$. Ένα διάνυσμα πιθανοτήτων $\boldsymbol{y}$ είναι k-*ομοιόμορφο* (k-uniform) αν κάθε y_i είναι ακέραιο πολλαπλάσιο του $1/k$.

(β) Έστω A πίνακας $m \times n$ με όλα τα στοιχεία του στο $[0,1]$ και έστω $\boldsymbol{x}$ ένα διάνυσμα πιθανοτήτων στο $[n]$. Έστω ακόμη $k(m,\varepsilon) = \lceil \ln(2m)/(2\varepsilon^2) \rceil + 1$. Να δείξετε ότι για κάθε $\varepsilon > 0$, υπάρχει ένα $k(m,\varepsilon)$-ομοιόμορφο διάνυσμα πιθανοτήτων $\boldsymbol{y}$ στο $[n]$ τέτοιο ώστε $\|A\boldsymbol{x} - A\boldsymbol{y}\|_\infty \le \varepsilon$.

Υπόδειξη: Να χρησιμοποιήσετε το ακόλουθο Hoeffding bound: Έστω $X_1, \dots, X_n$ ανεξάρτητες τυχαίες μεταβλητές στο $[0,1]$, και έστω $X = \left(\sum_{i=1}^n X_i\right)/n$. Για κάθε $\varepsilon > 0$, $\mathbb{P}\mathrm{r}[|X - \mathbb{E}\mathrm{xp}[X]| > \varepsilon] \le 2e^{-2n\varepsilon^2}$.

Άσκηση 2 (Linear Integer Programming Formulations). Να διατυπώσετε τα παρακάτω προβλήματα βελτιστοποίησης ως προβλήματα ακέραιου γραμμικού προγραμματισμού (αρκεί να δώσετε τα formulations, δεν χρειάζεται να εξηγήσετε αναλυτικά πως καταλήξατε σε αυτά):

(α) Έστω σύνολο σημείων C σε έναν μετρικό χώρο και $k \le |C|$. Δίνονται οι αποστάσεις $d : C \times C \to \mathbb{N}$ για κάθε ζευγάρι σημείων $(i,j) \in C \times C$. Επιλέγουμε k κέντρα από το C, δηλ. υποσύνολο $S \subseteq C$, με $|S| = k$, και αναθέτουμε κάθε σημείο $x \in C$ στο πλησιέστερο κέντρο $\mathrm{center}(x) = \arg\min_{y \in S} d(x,y)$. Για κάθε $y \in S$, έστω $r(y) = \max_{x:\mathrm{center}(x)=y} d(x,y)$ η "ακτίνα" του cluster σημείων που ανατίθενται στο y. Ζητείται να επιλέξουμε $S \subseteq C$, με $|S| = k$, που ελαχιστοποιεί το άθροισμα των "ακτινών" $r(y)$, δηλ. την ποσότητα $\sum_{y \in S} r(y)$.

(β) Δίνονται σύνολο C με τις θέσεις n πελατών και σύνολο F με m πιθανές θέσεις καταστημάτων. Δίνονται ακόμη το κόστος $f_j \in \mathbb{N}$ για να ανοίξουμε κατάστημα σε κάθε θέση $j \in F$ και οι αποστάσεις $d : C \times F \to \mathbb{N}$ για κάθε ζευγάρι θέσεων $(i,j) \in C \times F$. Ζητείται υποσύνολο $F' \subseteq F$ θέσεων όπου θα ανοίξουμε καταστήματα, ώστε να ελαχιστοποιήσουμε το άθροισμα του συνολικού κόστους για να ανοίξουμε καταστήματα στις θέσεις του F' και της συνολικής απόσταση κάθε πελάτη $i \in C$ από το κοντινότερό του ανοικτό κατάστημα.

Άσκηση 3 (Partial Vertex Cover). Δίνονται γράφημα $G(V,E)$ και παράμετρος $\beta > 0$. Ζητείται υποσύνολο κορυφών $C \subseteq V$ που ελαχιστοποιεί το $\beta|C| + |U(C)|$, όπου $U(C) = \{\{u,v\} \in E : u, v \notin C\}$ είναι οι ακμές που δεν καλύπτονται από το C.

(α) Να διατυπώσετε το παραπάνω πρόβλημα ως πρόβλημα (γραμμικού) ακέραιου προγραμματισμού, να δώσετε το αντίστοιχο LP relaxation, και να βρείτε το αντίστοιχο δυϊκό γραμμικό πρόγραμμα. Να διατυπώσετε το πρόβλημα βελτιστοποίησης που περιγράφεται από το δυϊκό πρόγραμμα σε φυσική γλώσσα.

(β) Με βάση το LP relaxation του (α), να διατυπώσετε προσεγγιστικό αλγόριθμο που βασίζεται σε deterministic rounding και να αναλύσετε τον λόγο προσέγγισης που επιτυγχάνει ο αλγόριθμός σας.

Άσκηση 4. Να λύσετε την [1, Άσκηση **5.3**] και την [1, Άσκηση **5.6**].

Άσκηση 5 (Number Theory). Έστω η ομάδα $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$, όπου $p > 2$ πρώτος αριθμός, και $p - 1 = 4q$, με q πρώτο αριθμό (π.χ. $p = 29, q = 7$).

(α) Ποια είναι η τάξη της ομάδας και ποιες οι δυνατές τάξεις των στοιχείων της ομάδας;

(β) Αν σας δώσουν έναν γεννήτορα g πώς μπορείτε να βρείτε ένα στοιχείο τάξης 4; (θεωρήστε γνωστό ότι η ομάδα είναι κυκλική) (γ) Διατυπώστε πιθανοτικό αλγόριθμο πολυωνυμικού χρόνου που με είσοδο p πρώτο (τ.ώ. $p - 1 = 4q$, q πρώτος) να βρίσκει γεννήτορα της $\mathbb{Z}_p^*$. Εξηγήστε την ορθότητα και την πολυπλοκότητα του αλγορίθμου σας.

Άσκηση 6 (Parameterized Algorithms)**.** Διατυπώστε παραμετρικό αλγόριθμο για το πρόβλημα Dominating Set με παράμετρο το μέγεθος του κυρίαρχου συνόλου. Είναι ο αλγόριθμός σας FPT; Εξηγήστε. Αλλάζει κάτι αν θεωρήσουμε ως παράμετρο και τον μέγιστο βαθμό του γράφου εισόδου Δ;

Άσκηση 7 (Group Theory, Bonus άσκηση (προαιρετική))**.** `https://courses.corelab.ntua.gr/pluginfile.php/494/mod_resource/content/2/BONUS_CRYPTO.pdf`

Σημείωση: αγνοήστε την ημερομηνία παράδοσης που αναγράφεται στην εκφώνηση.

Αναφορές

[1] D.P. Williamson and D.B. Shmoys. *The Design of Approximation Algorithms*. Cambridge University Press, 2010.