Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Θεμελιώδη Θέματα Επιστήμης Υπολογιστών, 2018-19

Επιμέλεια ασκήσεων: Ε. Ζάχος, Α. Παγουρτζής, Θ. Σούλιου, Α. Χαλκή

2η σειρά γραπτών ασκήσεων

(τυπικές γλώσσες – γραμματικές – αλγοριθμικές τεχνικές αναγωγές – κρυπτογραφία)

Άσκηση 1.

Ποιά από τα παρακάτω σύνολα είναι κανονικά και ποια όχι; Αποδείξτε!

α) $\{0^i 1^j \mid i, j \geq 1 \text{ και } i \neq j\}$

β) $\{a^n b^m \mid n \text{ είναι τέλειο τετράγωνο}\}$

γ) $\{1^{2k} 0^{j+1} \mid k \geq 1 \text{ και } j \geq 0\}$

δ) $\{0^{k+2} 1^k 0^{k-2} \mid k \geq 1\}$

Άσκηση 2.

(α) Έστω $G : S \to aS \mid aSbS \mid \varepsilon$. Αποδείξτε:
$L(G) = \{x \mid$ κάθε πρόθεμα του x έχει τουλάχιστον τόσα a όσα $b\}$.

(β) Δώστε γραμματική για τη γλώσσα $\{a^{3n} b^{2n} \mid n \geq 1\}$.

(γ) Δώστε γραμματική για τη γλώσσα $\{w \in \{0,1\}^* \mid$ το w έχει περιττό μήκος και (ακριβώς) στη μέση $111\}$.

Άσκηση 3.

(α) Αποδείξτε ότι η κλάση των κανονικών γλωσσών είναι κλειστή[1] ως προς την πράξη της **αναστροφής**: $L^R = \{w^R \mid w \in L\}$ π.χ. αν $L = \{001, 01011\}$, τότε $L^R = \{100, 11010\}$.

(β) Αποδείξτε ότι η κλάση των γλωσσών χωρίς συμφραζόμενα είναι κλειστή ως προς την πράξη **ένωση** και **άστρο του Kleene**. Τι έχετε να πείτε για τις πράξεις της **αναστροφής** και του **συμπληρώματος**;

Υπόδειξη: υποθέστε ότι για γλώσσες L_1, L_2 έχουμε γραμματικές χωρίς συμφραζόμενα και σκεφτείτε αν και πώς μπορούμε να βρούμε γραμματικές χ.σ. και για τις $L_1 \cup L_2,\ L_1^*, L_1^R$ και $\bar{L}_1$.

Εξάσκηση

Εξασκηθείτε στο σχεδιασμό και κατανόηση λειτουργίας των DFA, NFA και NFA$_\varepsilon$ χρησιμοποιώντας το εργαλείο που θα βρείτε στη σελίδα `http://automata.discrete.gr/` (Ευχαριστίες στους δημιουργούς, απόφοιτους της ΣΗΜΜΥ, Μανόλη Ζαμπετάκη και Διονύση Ζήνδρο).

Επαληθεύστε την ορθή λειτουργία των αυτομάτων που σχεδιάσατε στις προηγούμενες ασκήσεις (όπου γίνεται) με χρήση του εργαλείου αυτού.

Προαιρετικά: ελάτε σε επαφή με τους δημιουργούς της εφαρμογής για να συμβάλετε στην ανάπτυξη νέων λειτουργιών ή/και βελτίωση του interface.

[1] Δηλαδή αν μία γλώσσα είναι κανονική, τότε και η ανάστροφή της είναι κανονική.

Άσκηση 4. (Αναδρομή – Επανάληψη – Επαγωγή)

(α) Εκφράστε τον αριθμό μετακινήσεων δίσκων που κάνει ο αναδρομικός αλγόριθμος για τους πύργους του Hanoi, σαν συνάρτηση του αριθμού των δίσκων n.

(β) Δείξτε ότι ο αριθμός μετακινήσεων του αναδρομικού ισούται με τον αριθμό μετακινήσεων του επαναληπτικού αλγορίθμου.

(γ) Δείξτε ότι ο αριθμός των μετακινήσεων των παραπάνω αλγορίθμων είναι ο ελάχιστος μεταξύ όλων των δυνατών αλγορίθμων για το πρόβλημα αυτό.

(δ)* Θεωρήστε το πρόβλημα των πύργων του Hanoi με 4 αντί για 3 πασσάλους. Σχεδιάστε αλγόριθμο μετακίνησης n δίσκων από τον πάσσαλο 1 στον πάσσαλο 4 ώστε το πλήθος των βημάτων να είναι σημαντικά μικρότερο από το πλήθος των βημάτων που απαιτούνται όταν υπάρχουν μόνο 3 πάσσαλοι. Εκφράστε τον αριθμό των απαιτούμενων βημάτων σαν συνάρτηση του n.

Άσκηση 5. (Λογική και Αλγόριθμοι)

Διατυπώστε αποδοτικό αλγόριθμο που να δέχεται σαν είσοδο οποιονδήποτε τύπο της προτασιακής λογικής σε διαζευκτική κανονική μορφή (DNF) και να αποφαίνεται αν είναι ικανοποιήσιμος. Σε περίπτωση που είναι θα πρέπει να επιστρέφει μία ανάθεση αληθοτιμών που ικανοποιεί τον τύπο.

Π.χ. με είσοδο $(x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_2 \wedge x_3) \vee (x_4 \wedge x_5 \wedge \neg x_6)$ θα πρέπει να επιστρέφει 'Ναι' και μία από τις αναθέσεις αληθοτιμών στις $(x_1, \ldots, x_6)$ που ικανοποιούν τον τύπο, π.χ. την ανάθεση $(\mathsf{True}, \mathsf{False}, \mathsf{True}, \mathsf{False}, \mathsf{False}, \mathsf{False})$ ενώ με είσοδο $(x_1 \wedge \neg x_1 \wedge x_2) \vee (\neg x_3 \wedge x_3)$ θα πρέπει να επιστρέφει 'Όχι'.

Θεωρήστε ότι όλες οι μεταβλητές ενός τύπου δίνονται στη μορφή x_n, όπου n ένας φυσικός αριθμός.

Άσκηση 6. (Αλγόριθμοι γράφων)

Θεωρήστε το εξής πρόβλημα σε κατευθυνόμενους γράφους: κάθε κόμβος έχει μια θετική ακέραια τιμή και θέλουμε για κάθε κόμβο u να βρεθεί ο κόμβος με την ελάχιστη τιμή που είναι προσβάσιμος από τον u (μπορεί να είναι και ο ίδιος ο u). Περιγράψτε όσο το δυνατόν πιο αποδοτικό αλγόριθμο για το πρόβλημα αυτό στις εξής περιπτώσεις:

(α) Ακυκλικοί γράφοι.

(β) Γενικοί γράφοι.

Άσκηση 7. (Δυναμικός προγραμματισμός)

Σε ένα εργοστάσιο υαλικών θέλουν να μετρήσουν την αντοχή των κρυστάλλινων ποτηριών που κατασκευάζουν. Συγκεκριμένα, θέλουν να βρουν ποιο ακριβώς (με ακρίβεια εκατοστού) είναι το μέγιστο ύψος από το οποίο μπορούν να πέσουν τα ποτήρια τους χωρίς να σπάσουν. Η διεύθυνση του εργοστασίου μπορεί να διαθέσει έως ένα πλήθος ποτηριών k για τις δοκιμές (δηλ. δέχεται να καταστραφούν k ποτήρια) και θέλει το μέγιστο πλήθος δοκιμών που θα χρειαστούν να είναι όσο το δυνατόν μικρότερο. Επιπλέον, είναι γνωστό ότι τα ποτήρια σίγουρα σπάνε από ένα δεδομένο ύψος n εκατοστών και πάνω και ότι όλα τα ποτήρια είναι της ίδιας ακριβώς αντοχής.

Με βάση τα παραπάνω δεδομένα σχεδιάστε αλγόριθμο που να βρίσκει την βέλτιστη σειρά δοκιμών, με είσοδο τα n και k έτσι ώστε να ελαχιστοποιείται το πλήθος των δοκιμών στη χειρότερη περίπτωση. Ειδικότερα:

(α) Βρείτε την βέλτιστη σειρά δοκιμών για $n = 100$ και $k = 1$, καθώς και για $n = 100$ και $k = 2$. Ποιό είναι το μέγιστο πλήθος δοκιμών που μπορεί να χρειαστεί η λύση σας; Γενικεύστε για οποιοδήποτε n

και $k = 2$.

(β)* Προσπαθήστε να γενικεύσετε για οποιαδήποτε n και k (*υπόδειξη*: προσπαθήστε αρχικά να εκφράσετε τη βέλτιστη λύση της περίπτωσης οποιουδήποτε n και $k = 2$ αναδρομικά, χρησιμοποιώντας λύσεις της περίπτωσης $k = 1$, και της περίπτωσης $k = 2$ για μικρότερα n).

Ποια είναι η πολυπλοκότητα του αλγορίθμου σας;

(γ)* Υλοποιήστε τον αλγόριθμό σας σε γλώσσα προγραμματισμού της επιλογής σας.

Άσκηση 8. (Αναγωγές προς απόδειξη δυσκολίας)

Κυρίαρχο σύνολο (Dominating Set) σε έναν γράφο $G(V, E)$ λέγεται ένα υποσύνολο V' των κόμβων του γράφου τέτοιο ώστε κάθε κόμβος του γράφου που δεν ανήκει στο V' έχει έναν τουλάχιστον γείτονα στο V', δηλαδή $\forall v \in V : v \in V' \vee \exists u \in V' : \{u, v\} \in E$.

Το πρόβλημα της Τοποθέτησης Πυροσβεστικών Σταθμών (Firestation Placement) περιγράφεται ως εξής: δίνεται ένα σύνολο πόλεων σε μια περιφέρεια και όλες οι μεταξύ τους αποστάσεις (σαν ακέραιοι αριθμοί). Δίνεται ακόμη ότι ο προϋπολογισμός της περιφέρειας επαρκεί για την εγκατάσταση k πυροσβεστικών σταθμών συνολικά που μπορούν να τοποθετηθούν σε κάποιες από τις πόλεις που θα επιλεγούν. Θέλουμε να τοποθετήσουμε τους σταθμούς κατά τέτοιον τρόπο που να εξυπηρετούνται όλες οι πόλεις όσο το δυνατόν καλύτερα. Συγκεκριμένα, θέλουμε κάθε πόλη να έχει έναν τουλάχιστον πυροσβεστικό σταθμό σε απόσταση το πολύ D, όπου D είναι ένας ακέραιος που επίσης δίνεται. Το ερώτημα είναι αν υπάρχει τρόπος τοποθέτησς των k σταθμών ώστε να ικανοποιείται η παραπάνω απαίτηση.

Περιγράψτε αναγωγή από το πρόβλημα Dominating Set (δίνεται γράφος και αριθμός k, υπάρχει κυρίαρχο σύνολο μεγέθους το πολύ k στο γράφο;) στο πρόβλημα Firestation Placement. Τι συμπέρασμα προκύπτει εάν γνωρίζουμε ότι το πρόβλημα Dominating Set είναι NP-πλήρες;

Υπόδειξη: χρησιμοποιήστε ιδέες από την αναγωγή του προβλήματος Hamilton Cycle στο Traveling Salesman Problem.

Άσκηση 9.* (Αριθμοί Fibonacci)

Συγκρίνετε την πολυπλοκότητα ψηφιοπράξεων (bit complexity) των δύο ταχύτερων αλγορίθμων για υπολογισμό αριθμών Fibonacci. Για τον αλγόριθμο με πίνακα θεωρήστε (α) απλό πολλαπλασιασμό ακεραίων και (β) πολλαπλασιασμό Gauss-Karatsuba. Τι παρατηρείτε;

Υλοποιήστε τους αλγορίθμους σε γλώσσα που να υποστηρίζει πολύ μεγάλους ακεραίους (100δων ψηφίων). Χρησιμοποιήστε τον πολλαπλασιασμό ακεραίων που παρέχει η γλώσσα. Τι συμπεραίνετε;

Άσκηση 10.* (Κρυπτογραφία)

(α) Γράψτε πρόγραμμα σε γλώσσα της επιλογής σας (θα πρέπει να υποστηρίζει πράξεις με αριθμούς 100δων ψηφίων) που να ελέγχει αν ένας αριθμός είναι πρώτος με τον έλεγχο (test) του Fermat:

Αν n πρώτος τότε για κάθε a τ.ώ. $1 < a < n - 1$, ισχύει

$$a^{n-1} \bmod n = 1$$

Αν λοιπόν, δεδομένου ενός n βρεθεί a ώστε να μην ισχύει η παραπάνω ισότητα τότε ο αριθμός n είναι οπωσδήποτε σύνθετος. Αν η ισότητα ισχύει, τότε το n είναι πρώτος με αρκετά μεγάλη πιθανότητα (για τους περισσότερους αριθμούς $\geq 1/2$). Για να αυξήσουμε σημαντικά την πιθανότητα μπορούμε να επαναλάβουμε μερικές φορές (τυπικά 30 φορές) με διαφορετικό a. Αν όλες τις φορές βρεθεί να

ισχύει η παραπάνω ισότητα τότε λέμε ότι το n "περνάει το test" και ανακηρύσσουμε το n πρώτο αριθμό·αν έστω και μία φορά αποτύχει ο έλεγχος, τότε ο αριθμός είναι σύνθετος.

Η συνάρτησή σας θα πρέπει να δουλεύει σωστά για αριθμούς χιλιάδων ψηφίων, π.χ. να μπορεί να ελέγξει αν ο αριθμός $n = 2^x - 1$ είναι πρώτος για κάθε $x < 2000$. Δοκιμάστε την για όλους τους αριθμούς της μορφής $n = 2^x - 1$ με x πρώτο και $x < 2000$ (αν το x δεν είναι πρώτος, ούτε το $2^x - 1$ είναι πρώτος – μπορείτε να το αποδείξετε;). Τι αποτελέσματα πήρατε;

Σημείωση 1: θυμηθείτε ότι το $a^{2^{1279}-2}$ έχει αστρονομικά μεγάλο πλήθος ψηφίων (δεν χωράει να γραφτεί σε ολόκληρο το σύμπαν!), ενώ το $a^{2^{1279}-2} \bmod (2^{1279} - 1)$ είναι σχετικά "μικρό" (έχει μερικές εκατοντάδες δεκαδικά ψηφία *μόνο* :-)).

Σημείωση 2: Υπάρχουν (λίγοι) σύνθετοι που έχουν την ιδιότητα να περνούν τον έλεγχο Fermat για κάθε a που είναι σχετικά πρώτο με το n, οπότε για αυτούς το test θα αποτύχει όσες δοκιμές και αν γίνουν (εκτός αν πετύχουμε κατά τύχη a που δεν είναι σχετικά πρώτο με το n, πράγμα αρκετά απίθανο). Αυτοί οι αριθμοί λέγονται *Carmichael* – δείτε και `http://en.wikipedia.org/wiki/Carmichael_number`. Ελέγξτε τη συνάρτησή σας με *αρκετά μεγάλους* αριθμούς Carmichael που θα βρείτε π.χ. στη σελίδα `http://de.wikibooks.org/wiki/Pseudoprimzahlen:_Tabelle_Carmichael-Zahlen`. Τι παρατηρείτε;

(β) Μελετήστε και υλοποιήστε τον έλεγχο Miller-Rabin που αποτελεί βελτίωση του ελέγχου του Fermat και δίνει σωστή απάντηση με πιθανότητα τουλάχιστον 1/2 για *κάθε* φυσικό αριθμό (οπότε με 30 επαναλήψεις έχουμε αμελητέα πιθανότητα λάθους για κάθε αριθμό εισόδου). Δοκιμάστε τον με διάφορους αριθμούς Carmichael. Τι παρατηρείτε;

Άσκηση 11.* (Αναγωγές προς απόδειξη δυσκολίας)

Έστω ένα μη κατευθυνόμενο γράφημα $G = (V, E)$. **Κλίκα** λέγεται ένα υπογράφημα του G το οποίο είναι πλήρες (δηλ. όλες οι κορυφές του ενώνονται με ακμή). Ένα σύνολο κορυφών του G λέγεται **ανεξάρτητο σύνολο** αν κάθε δύο κορυφές του δε συνδέονται με ακμή. Θεωρήστε τα προβλήματα απόφασης: (i) **Independent Set**, το οποίο δεδομένης εισόδου (G, k) έχει θετική απάντηση αν και μόνο αν το γράφημα G περιέχει κάποιο ανεξάρτητο σύνολο μεγέθους τουλάχιστον k, (ii) **Clique**, το οποίο δεδομένης εισόδου (G, k) έχει θετική απάντηση μεγέθους τουλάχιστον k και (iii) **Dense Subgraph**, το οποίο δεδομένου ενός γραφήματος G και δύο θετικών ακέραιων a, b έχει θετική απάντηση αν και μόνο αν το G περιέχει ένα σύνολο κορυφών μεγέθους a έτσι ώστε να υπάρχουν τουλάχιστον b ακμές μεταξύ τους.

(α) Δείξτε ότι αν είναι γνωστό ότι το πρόβλημα **Independent Set** είναι NP-πλήρες, τότε και το πρόβλημα **Clique** είναι NP-πλήρες.

(β) Δείξτε επίσης ότι το πρόβλημα **Dense Subgraph** είναι NP-πλήρες.

Προθεσμία υποβολής και οδηγίες. Οι απαντήσεις θα πρέπει να υποβληθούν έως τις 30/11/2018, στις 23:59, σε ηλεκτρονική μορφή, στο mycourses (φροντίστε το τελικό αρχείο να είναι μεγέθους <2MB συνολικά).

Τα ερωτήματα με (*) είναι προαιρετικά. Εφ'όσον τα επιλύσετε μπορούν να προσμετρηθούν στη θέση ερωτημάτων που δεν απαντήσατε.

Συνιστάται *θερμά* να αφιερώσετε ικανό χρόνο για να λύσετε τις ασκήσεις μόνοι σας προτού καταφύγετε σε οποιαδήποτε *θεμιτή* βοήθεια (διαδίκτυο, βιβλιογραφία, συζήτηση με συμφοιτητές). Σε κάθε περίπτωση, οι απαντήσεις θα πρέπει να είναι *αυστηρά* ατομικές (δηλαδή όχι 'copy-paste').

Για να βαθμολογηθείτε θα πρέπει να παρουσιάσετε σύντομα τις λύσεις σας σε ημέρα και ώρα που θα ανακοινωθεί αργότερα.

Για απορίες / διευκρινίσεις: στείλτε μήνυμα στη διεύθυνση `focs@corelab.ntua.gr`.