Πανεπιστημιο Αθηνων, Υπολογιστικη Πολυπλοκοτητα
Εαρινο εξαμηνο 2010-2011, Δευτερο Συνολο Ασκησεων
Δημοσιευση: 11 Μαιου 2011
Παραδοση: 31 Μαιου 2011, ωρα 12:00

Η ΗΜΕΡΟΜΗΝΙΑ ΚΑΙ Η ΩΡΑ ΠΑΡΑΔΟΣΗΣ ΕΙΝΑΙ ΑΝΕΛΑΣΤΙΚΕΣ.

Είναι *χρήσιμο* να συζητάτε μεταξύ σας τα προβλήματα. Το γράψιμο των απαντήσεων πρέπει να είναι ***αυστηρά ατομική*** υπόθεση.

Πρόβλημα 1 [2 μονάδες]. Ορίστε τη γλώσσα Fbit ως το σύνολο των ζευγών $< x, i >$ όπου $x, i \in \mathbb{N}$ τέτοιοι ώστε το iοστό bit του μεγαλύτερου πρώτου παράγοντα του x είναι ίσο με 1.
(1) Γνωρίζοντας πως Primes $\in \mathcal{P}$, δείξτε πως Fbit $\in \mathcal{NP} \cap co\mathcal{NP}$.
(2) Αποδείξτε πως αν $\mathcal{P} = \mathcal{NP} \cap co\mathcal{NP}$, Factoring $\in \mathcal{FP}$.
Factoring είναι η συνάρτηση που υπολογίζει την παραγοντοποίηση ενός αριθμού x σε γινόμενο πρώτων παραγόντων.

Πρόβλημα 2 [4 μονάδες]. Πρόβλημα 10.4.6 από τον Παπαδημητρίου: Strong nondeterministic Turing machines.

Πρόβλημα 3 [4 μονάδες]. Θεωρείστε τον παρακάτω ορισμό του $\mathcal{P}$/poly.

> **Ορισμός $\mathcal{P}$/poly.** $L \in \mathcal{P}/\text{poly}$ if there exists a polynomial-time Turing machine M, a polynomial $p()$ and a function h mapping numbers to strings, where $|h(n)| \leq p(n)$, such that for all strings x
>
> $$x \in L \Leftrightarrow < x, h(|x|) > \text{ is accepted by } M.$$

(1) Αποδείξτε πως είναι ισοδύναμος με τον ορισμό μέσω κυκλωμάτων.
(2) Θυμηθείτε τον ορισμό του $\mathcal{NP}$.

> **Ορισμός $\mathcal{NP}$.** $L \in \mathcal{NP}$ if there exists a polynomial-time Turing machine M and a polynomial $p()$ such that for all strings x
>
> $$x \in L \Leftrightarrow \exists y \text{ s.t. } |y| \leq p(|x|) \text{ and } < x, y > \text{ is accepted by } M.$$

Μια προφανής διαφορά ανάμεσα στους δύο ορισμούς είναι πως για δύο x ίδιου μήκους, στο δεύτερο ορισμό μπορεί τα αντίστοιχα πιστοποιητικά y να είναι διαφορετικά. Αυτό όμως δεν φαίνεται να αρκεί για να αποκλείσουμε το γεγονός πως ο ορισμός του $\mathcal{P}$/poly είναι ειδική περίπτωση του ορισμού του $\mathcal{NP}$. (Το οποίο θα σήμαινε πως $\mathcal{P}/\text{poly} \subseteq \mathcal{NP}$.) Ποια είναι η κρίσιμη διαφορά ανάμεσα στους δύο ορισμούς;

Πρόβλημα 4 [4 μονάδες]. Αποδείξτε τη συνεπαγωγή $\mathcal{P} = \mathcal{NP} \Rightarrow \mathcal{EXP} = \mathcal{NEXP}$. *Υπόδειξη:* δοκιμάστε να «φουσκώσετε» τη συμβολοσειρά εισόδου.

Πρόβλημα 5 [4 μονάδες]. Δείξτε πως τα ακόλουθα προβλήματα είναι $\mathcal{NP}$-complete.
1) Δίνονται μη κατευθυνόμενα γραφήματα G, H. Είναι το H ισόμορφο με υπογράφημα του G;
2) Δίνεται μη κατευθυνόμενο γράφημα $G = (V, E)$. Περιέχει το G μονοπάτι με τουλάχιστον $|V|/2$ κόμβους;

Πρόβλημα 6 [4 μονάδες]. Στο πρόβλημα Feedback Arc Set, δίνεται ένα κατευθυνόμενο γράφημα $G = (V, A)$ και ζητάμε ένα υποσύνολο $A' \subseteq A$ τέτοιο ώστε το $G = (V, A \setminus A')$ να είναι άκυκλο και το μέγεθος του A' να είναι ελάχιστο. Αποδείξτε πως το αντίστοιχο πρόβλημα απόφασης είναι $\mathcal{NP}$-complete. Τί συμβαίνει αν το γράφημα είναι μη κατευθυνόμενο;

Πρόβλημα 7 [2 μονάδες]. Ορίζουμε την κλάση πολυπλοκότητας $\mathcal{NR}$.
Μια γλώσσα $L \in \mathcal{NR}$, αν υπάρχει πιθανοτικός πολυωνυμικός αλγόριθμος V, και πολυώνυμο $p(n)$ τέτοια ώστε
1) για κάθε $x \in L$, υπάρχει $y \in \{0,1\}^{p(n)}$, έτσι ώστε $Pr[V(x,y) = \text{yes}] \geq 1/2$, και
2) για κάθε $x \notin L$, και για κάθε y, $Pr[V(x,y) = \text{no}] = 1$.

Μπορείτε να συσχετίσετε το $\mathcal{NR}$ με κάποια γνωστή κλάση;

Πρόβλημα 8 [6 μονάδες]. Έστω $L \in NSPACE(s(n))$, $s(n) = \Omega(\log n)$. Αποδείξτε πως υπάρχει πιθανοτική Μ. Τ. M η οποία τρέχει σε χώρο $O(s(n))$ και (i) αν $x \in L$, $M(x) = yes$ με πιθανότητα τουλάχιστον $1/2$ και (ii) αν $x \notin L$, $M(x) = no$ με πιθανότητα 1.

Υπόδειξη: δεν μας ενδιαφέρει ο χρόνος εκτέλεσης της M, αρκεί να τερματίζει.