



Θεωρητική Πληροφορική Ι - Υπολογιστική Πολυπλοκότητα 2η Σειρά Ασκήσεων

Διδάσκοντες: Σ. Ζάχος, Α. Παγουρτζής
Χειμερινό Εξάμηνο 2018-2019

Η παράδοση της εργασίας:

-γίνεται ηλεκτρονικά στο [moodle](#) του μαθήματος (παράδοση με e-mail δεν θα γίνει αποδεκτή)
-πρέπει να γίνει μέχρι και την 7/1/2019.

Είναι αποδεκτό (και σε ορισμένες ασκήσεις απαραίτητο) να αναζητήσετε την βιβλιογραφία, είναι όμως απαραίτητο να παραθέσετε αναφορές για οτιδήποτε χρησιμοποιήσετε.

Η μη αναφορά των πηγών συνιστά λογοκλοπή, πρακτική ακαδημαϊκά ανεπίτρεπτη με συνέπειες στην βαθμολόγηση της εργασίας.

Άσκηση 1

Δείξτε ότι αν $\text{DSPACE}[n] \subseteq \mathbf{P}$, τότε $\mathbf{P} = \mathbf{PSPACE}$.

Υπόδειξη: Χρησιμοποιήστε padding.

Άσκηση 2

Έστω γλώσσα $L \subseteq \Sigma^*$ και κλάση πολυπλοκότητας \mathcal{C} . Η L ονομάζεται “low” για την \mathcal{C} αν $\mathcal{C}^L = \mathcal{C}$. Αυτό διαισθητικά σημαίνει ότι η γλώσσα L δεν προσφέρει επιπλέον υπολογιστική δύναμη στην \mathcal{C} αν την χρησιμοποιήσουμε ως μαντείο (oracle). Επιπλέον, για δύο κλάσεις πολυπλοκότητας \mathcal{C} και \mathcal{C}' λέμε ότι η \mathcal{C}' είναι low για την \mathcal{C} αν για κάθε $L \in \mathcal{C}'$: $\mathcal{C}^L = \mathcal{C}$. Δείξτε ότι:

1. $\mathbf{P}^{\text{BPP}} = \mathbf{BPP}$.
2. Η \mathbf{BPP} είναι low για την \mathbf{PP} .

Άσκηση 3

Θεωρώντας δεδομένο ότι $\mathbf{ZPP} = \mathbf{RP} \cap \text{coRP}$, δείξτε ότι μια γλώσσα $L \in \mathbf{ZPP}$ αποφασίζεται σε χρόνο $T(n)$ από μία Πιθανοτική Μηχανή Turing που δίνει πάντοτε σωστή απάντηση, και ισχύει:

$$\mathbb{E}[T(n)] \leq 2(p_1(n) + p_2(n))$$

όπου n το μήκος της εισόδου, $p_1(n), p_2(n)$ τα πολυώνυμα που φράσσουν τους χρόνους εκτέλεσης της \mathbf{RP} και coRP μηχανής αντίστοιχα, και το “ $\mathbb{E}[\cdot]$ ” συμβολίζει την μέση ή αναμενόμενη τιμή μιας τυχαίας μεταβλητής.

Άσκηση 4

Θα μελετήσουμε τον τελεστή “ $\mathcal{BP} \cdot$ ”, που δρα πάνω σε κλάσεις πολυπλοκότητας, και τις ιδιότητές του:

Ορισμός 1. Έστω \mathbf{C} μια κλάση πολυπλοκότητας και $L \subseteq \Sigma^*$. $L \in \mathcal{BP} \cdot \mathbf{C}$ αν υπάρχει μία γλώσσα $A \in \mathbf{C}$, ένα πολυώνυμο p , και μία σταθερά $\varepsilon > 0$ τέτοιο ώστε για κάθε $x \in \Sigma^*$:

$$\Pr_{y \in \{0,1\}^{p(|x|)}} [(x; y) \in A \leftrightarrow x \in L] \geq \frac{1}{2} + \varepsilon$$

1. Δείξτε ότι $\mathcal{BP} \cdot \mathbf{P} = \mathbf{BPP}$.
2. Δείξτε ότι αν $\mathbf{C}_1 \subseteq \mathbf{C}_2$, τότε και $\mathcal{BP} \cdot \mathbf{C}_1 \subseteq \mathcal{BP} \cdot \mathbf{C}_2$.
3. Δείξτε ότι $co(\mathcal{BP} \cdot \mathbf{C}) \subseteq \mathcal{BP} \cdot (co\mathbf{C})$. Τι συνεπάγεται αυτή η σχέση αν η \mathbf{C} είναι κλειστή ως προς συμπλήρωμα?
4. Δείξτε ότι αν η \mathbf{C} είναι κλειστή ως προς padding¹ τότε $\mathbf{C} \subseteq \mathcal{BP} \cdot \mathbf{C}$.

όπου $\mathbf{C}, \mathbf{C}_1, \mathbf{C}_2$ κλάσεις πολυπλοκότητας.

Άσκηση 5

Δείξτε ότι η συνάρτηση $PARITY(x_1, x_2, \dots, x_n) = (\sum_{i=1}^n x_i \pmod{2}) \in \mathbf{NC}^1$.

Άσκηση 6 (Bonus)

Ορίζουμε την κλάση S_2^p ως το σύνολο των γλωσσών L για τις οποίες υπάρχει ένα πολυωνυμικά υπολογίσιμο και ισορροπημένο κατηγορημα R , τέτοιο ώστε:

- $x \in L \Rightarrow \exists y \forall z R(x, y, z) = 1$
- $x \notin L \Rightarrow \exists z \forall y R(x, y, z) = 0$

όπου $|y| \leq p(|x|)$, $|z| \leq q(|x|)$ (Το “ S ” προκύπτει από το Symmetric). Το παραπάνω σημαίνει ότι υπάρχουν δύο “provers” που παρέχουν πιστοποιητικά: Αν $x \in L$, υπάρχει πιστοποιητικό y (που παρέχει ο πρώτος prover), που ανεξάρτητα από το πιστοποιητικό του δεύτερου, η ΤΜ αποδέχεται, και ομοίως για την περίπτωση όπου $x \notin L$, υπάρχει πιστοποιητικό z (που παρέχει ο δεύτερος), που ανεξάρτητα από το πιστοποιητικό του πρώτου, η ΤΜ απορρίπτει.

1. Δείξτε ότι $\mathbf{NP} \cup co\mathbf{NP} \subseteq S_2^p \subseteq \Sigma_2^p \cap \Pi_2^p$.
2. Ορίζουμε τον αντίστοιχο τελεστή \mathcal{S}_2 , έτσι ώστε $S_2^p = \mathcal{S}_2 \cdot \mathbf{P}$, και φυσιολογικά δημιουργείται η ιεραρχία κλάσεων $S_{2k}^p = \underbrace{\mathcal{S}_2 \cdot \mathcal{S}_2 \cdots \mathcal{S}_2}_k \cdot \mathbf{P}$. Δείξτε ότι $\Sigma_k^p \cup \Pi_k^p \subseteq S_{2k}^p \subseteq \Sigma_{2k}^p \cap \Pi_{2k}^p$.
3. Δείξτε ότι η ιεραρχία αυτή καταρρέει αν και μόνο αν η πολυωνυμική ιεραρχία καταρρέει.
4. Θεωρώντας δεδομένο ότι η κλάση S_2^p είναι κλειστή ως προς αναγωγές Cook, δείξτε ότι $\Delta_2^p \subseteq S_2^p$.

¹Μία κλάση είναι κλειστή ως προς padding αν $L \in \mathbf{C} \Rightarrow \{x; y | x \in L \wedge y \in \{0,1\}^*\} \in \mathbf{C}$.