Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών
Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών
Εργαστήριο Λογικής και Επιστήμης Υπολογισμών

Θεωρητική Πληροφορική Ι - Υπολογιστική Πολυπλοκότητα
Σειρά Ασκήσεων

Διδάσκοντες: Σ. Ζάχος, Ά. Παγουρτζής
Χειμερινό Εξάμηνο 2017-2018

Η παράδοση της εργασίας:
-γίνεται ηλεκτρονικά στο *moodle* του μαθήματος (παράδοση με e-mail δεν θα γίνει αποδεκτή)
-πρέπει να γίνει μέχρι και τις 15/3/2018.

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

α΄. Δείξτε ότι **NP** $\neq$ **DSPACE**$[n]$.
Υπόδειξη: Δεν γνωρίζουμε αν κάποια από τις δύο κλάσεις περιέχει την άλλη. Προσπαθήστε να αποδείξετε το ζητούμενο χρησιμοποιώντας κάποια ιδιότητα κλειστότητας που έχει μόνο μία από τις δύο κλάσεις.

β΄. Δείξτε ότι η κλάση **NP** είναι κλειστή ως προς τις logspace και τις Karp αναγωγές. Ισχύει το ίδιο και για την κλάση **DTIME**$[n^2]$;

Άσκηση 2

Δείξτε ότι αν η γλώσσα $L \subseteq \Sigma^*$ είναι πεπερασμένη, τότε $L \in$ **DTIME**$[n]$.

Άσκηση 3

Ο S. Cook όρισε μια διαφορετική αναγωγή από αυτές που χρησιμοποιούμε για τα **NP**-complete προβλήματα (αναγωγές κατά Karp, συμβ. $\leq_m^p$): Μια γλώσσα L ανάγεται σε πολυωνυμικό χρόνο κατά Cook (Cook reducible) σε μία γλώσσα L' (συμβ. $L \leq_T^P L'$) αν υπάρχει μία ΤΜ πολυωνυμικού-χρόνου με μαντείο την L', που αποφασίζει την L μετά από το πολύ πολυωνυμικές κλήσεις στο μαντείο.

α΄. Δείξτε ότι η αναγωγή κατά Cook είναι μεταβατική σχέση, δηλαδή: $L_1 \leq_T^P L_2 \wedge L_2 \leq_T^P L_3 \Rightarrow L_1 \leq_T^P L_3$.

β΄. Δείτε ότι $L \leq_m^p L' \Rightarrow L \leq_T^P L'$.

γ΄. Δείξτε ότι αν η **NP** είναι κλειστή ως προς την αναγωγή κατά Cook, τότε **NP** $= co$**NP**.

Άσκηση 4

α΄. Δείξτε ότι ο ορισμός με πιστοποιητικά της κλάσης **NL** (Ορισμός 4.19 από το βιβλίο των Arora-Barak [2]) είναι ισοδύναμος με τον αρχικό ορισμό της **NL** (**NL** $=$ **NSPACE**$[\log n]$).

β΄. Δείξτε ότι αν στον ορισμό με πιστοποιητικά της **NL** επιτρέψουμε στην read-once κεφαλή να κινείται και στις δύο κατευθύνσεις, τότε η κλάση που ορίζεται είναι ακριβώς η **NP**.

Άσκηση 5

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

Άσκηση 6

Θεωρώντας δεδομένο ότι **ZPP** $=$ **RP** $\cap$ *co***RP**, δείξτε ότι μια γλώσσα $L \in$ **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 **RP** και *co***RP** μηχανής αντίστοιχα, και το "$\mathbb{E}[\,\cdot\,]$" συμβολίζει την μέση ή αναμενόμενη τιμή μιας τυχαίας μεταβλητής.

Άσκηση 7

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

Ορισμός 1. *Έστω* **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* $x \in \Sigma^*$*:*

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

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 **C** είναι κλειστή ως προς συμπλήρωμα?
4. Δείξτε ότι αν η **C** είναι κλειστή ως προς padding[1] τότε $\mathbf{C} \subseteq \mathcal{BP} \cdot \mathbf{C}$.

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

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

Άσκηση 8

1. Δείξτε ότι $\mathbf{PCP}[0, \log n] = \mathbf{P}$.
2. Δείξτε ότι $\mathbf{PCP}[\log n, 1] \subseteq \mathbf{NP}$.
3. (*Bonus*) Έστω το πρόβλημα `GNI` (Graph non-isomorphism), που δοθέντων δύο γράφων εξετάζει αν *δεν* είναι ισομορφικοί. Δείξτε ότι:

$$\texttt{GNI} \in \mathbf{PCP}[n \log n, 1]$$

(*Υπενθυμίζουμε ότι δύο γράφοι $G = (V, E)$ και $G' = (V', E')$ λέγονται ισομορφικοί αν υπάρχει μία μετάθεση $\pi : V \to V'$ τέτοια ώστε $(\pi(u), \pi(v)) \in E'$ αν και μόνο αν $(u, v) \in E$.*)

Άσκηση 9

Μια γλώσσα $L \subseteq \{0,1\}^*$ λέγεται sparse (αραιή) αν έχει το πολύ πολυωνυμικά στοιχεία σε κάθε μήκος string, δηλαδή αν $|L \cap \{0,1\}^n| \leq p(n)$, για κάθε $n \in \mathbb{N}$, και p πολυώνυμο. Έστω **SPARSE** η κλάση των sparse γλωσσών. Δείξτε ότι $\mathbf{SPARSE} \subseteq \mathbf{P}_{/\mathbf{poly}}$.

Άσκηση 10

1. Ένα μη-ντετερμινιστικό κύκλωμα C έχει δύο εισόδους $x = x_1 x_2 \cdots x$ και $y = y_1 y_2 \cdots y_m$. Το κύκλωμα C αποδέχεται το x αν και μόνο αν $\exists y\ C(x, y) = 1$. Δείξτε ότι κάθε γλώσσα στην κλάση **MA** έχει μη-ντετερμινιστικά κυκλώματα πολυωνυμικού μεγέθους.
2. Δείξτε ότι $\mathcal{BP} \cdot co\mathbf{NP} = co\mathbf{AM}$.

Άσκηση 11

Δείξτε ότι $\mathbf{P}^{\mathbf{PP}} = \mathbf{P}^{\#\mathbf{P}}$.

Άσκηση 12

Ένα βασικό μειονέκτημα της κλάσης **#P** είναι ότι δεν περιλαμβάνει αρνητικές συναρτήσεις. Θα προσπαθήσουμε να επεκτείνουμε την κλάση **#P**, ως εξής:

Έστω $\#acc_M(x)$ ο αριθμός των accepting μονοπατιών μιας NTM . Ως γνωστόν, μια συνάρτηση $f : \Sigma^* \to \mathbb{N}$ ανήκει στην **#P** αν υπάρχει μία **NP** TM M τέτοια ώστε για κάθε $x \in \Sigma^*$, $f(x) = \#acc_M(x)$. Αντίστοιχα ορίζουμε την κλάση **GapP**: Μία συνάρτηση $f : \Sigma^* \to \mathbb{Z}$ ανήκει στην **GapP** αν υπάρχει μία **NP** TM M τέτοια ώστε για κάθε $x \in \Sigma^*$, $f(x) = \#acc_M(x) - \#rej_M(x)$, δηλαδή αν η συνάρτηση f ισούται με την διαφορά του πλήθους των accepting και του πλήθους των rejecting μονοπατιών.

1. Δείξτε ότι αν $f \in \mathbf{GapP}$, τότε και $-f \in \mathbf{GapP}$.
2. Δείξτε ότι $\#\mathbf{P} \subseteq \mathbf{GapP}$.
3. Δείξτε ότι τα επόμενα είναι ισοδύναμα:

   (α′) $f \in \mathbf{GapP}$.

(β΄) Η f μπορεί να γραφεί ως η διαφορά δύο #**P** συναρτήσεων.

(γ΄) Η f μπορεί να γραφεί ως η διαφορά μιας #**P** και μιας **FP** συνάρτησης.

4. Χρησιμοποιώντας τα παραπάνω, δείξτε ότι **GapP** $\subseteq$ **FP**$^{\#\mathbf{P}[1]}$.

Άσκηση Bonus

Ορίζουμε την κλάση S_2^p ως το σύνολο των γλωσσών L για τις οποίες υπάρχει ένα πολυωνυμικά υπολογίσιμο και ισορροπημένο κατηγόρημα 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 **NP** $\cup$ *co***NP** $\subseteq S_2^p \subseteq \Sigma_2^p \cap \Pi_2^p$.
2. Ορίζουμε τον αντίστοιχο τελεστή $\mathcal{S}_2 \cdot$, έτσι ώστε $S_2^p = \mathcal{S}_2 \cdot \mathbf{P}$, και φυσιολογικά δημιουργείται η ιεραρχία κλάσεων $S_{2k}^p = \underbrace{\mathcal{S}_2 \cdot \mathcal{S}_2 \cdot \cdots \mathcal{S}_2 \cdot}_{k} \mathbf{P}$. 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 $\Delta_2^p \subseteq S_2^p$.