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

Αλγόριθμοι & Πολυπλοκότητα ΙΙ
3η Σειρά Ασκήσεων

Διδάσκοντες: Σ. Ζάχος, Ά. Παγουρτζής
Χειμερινό Εξάμηνο 2014-2015

Η παράδοση της εργασίας:
-γίνεται ηλεκτρονικά στο *moodle* του μαθήματος (παράδοση με e-mail δεν θα γίνει αποδεκτή)
-πρέπει να γίνει μέχρι και τις 1/3/2015.

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

Έστω **SPARSE** η κλάση των sparse γλωσσών. Υπενθυμίζουμε ότι 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. Δείξτε ότι $\mathbf{SPARSE} \subseteq \mathbf{P_{/poly}}$.

Άσκηση 2

1. Ένα μη-ντετερμινιστικό κύκλωμα C έχει δύο εισόδους $x = x_1x_2\cdots x_n$ και $y = y_1y_2\cdots y_m$. Το κύκλωμα C αποδέχεται το x αν και μόνο αν $\exists y\ C(x,y) = 1$. Δείξτε ότι κάθε γλώσσα στο **MA** έχει μη-ντετερμινιστικά κυκλώματα πολυωνυμικού μεγέθους.

2. Δείξτε ότι $\mathcal{BP} \cdot co\mathbf{NP} = co\mathbf{AM}$.

Άσκηση 3

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 TM 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 TM 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 $\mathcal{S}_2\cdot$, έτσι ώστε $S_2^p = \mathcal{S}_2 \cdot \mathbf{P}$, και φυσιολογικά δημιουργείται η ιεραρχία κλάσεων $S_{2k}^p = \underbrace{\mathcal{S}_2 \cdot \mathcal{S}_2 \cdots \mathcal{S}_2 \cdot}_{k} \mathbf{P}$. 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 $\Delta_2^p \subseteq S_2^p$.

Άσκηση 4

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

Άσκηση 5

Ένα βασικό μειονέκτημα της κλάσης $\#\mathbf{P}$ είναι ότι δεν περιλαμβάνει αρνητικές συναρτήσεις. Θα προσπαθήσουμε να επεκτείνουμε την κλάση $\#\mathbf{P}$, ως εξής:
Έστω $\#acc_M(x)$ ο αριθμός των accepting μονοπατιών μιας NTM M. Ως γνωστόν, μια συνάρτηση $f : \Sigma^* \to \mathbb{N}$ ανήκει στην $\#\mathbf{P}$ αν υπάρχει μία $\mathbf{NP}$ TM M τέτοια ώστε για κάθε $x \in \Sigma^*$, $f(x) = \#acc_M(x)$.
Αντίστοιχα ορίζουμε την κλάση $\mathbf{GapP}$: Μία συνάρτηση $f : \Sigma^* \to \mathbb{Z}$ ανήκει στην $\mathbf{GapP}$ αν υπάρχει μία $\mathbf{NP}$ 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 $\#\mathbf{P}$ συναρτήσεων.

   (γ΄) Η f μπορεί να γραφεί ως η διαφορά μιας $\#\mathbf{P}$ και μιας $\mathbf{FP}$ συνάρτησης.

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