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

# Θεωρητική Πληροφορική Ι - Υπολογιστική Πολυπλοκότητα
# 2η Σειρά Ασκήσεων

Διδάσκοντες: Σ. Ζάχος, Ά. Παγουρτζής
Χειμερινό Εξάμηνο 2019-2020

**Η παράδοση της εργασίας:**
**-γίνεται ηλεκτρονικά στο *moodle* του μαθήματος (παράδοση με e-mail δεν θα γίνει αποδεκτή)**
**-πρέπει να γίνει μέχρι και την 7/3/20.**

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

## Άσκηση 2

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* $x \in \Sigma^*$*:*

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

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 padding[1] τότε $\mathbf{C} \subseteq \mathcal{BP} \cdot \mathbf{C}$.

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

## Άσκηση 3

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

## Άσκηση 4

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 5

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 6

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

*Υπόδειξη*: Χρησιμοποιήστε padding.

## Άσκηση 7 (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:

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

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

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 $\Delta_2^p \subseteq S_2^p$.