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

Προχωρημένα Θέματα Αλγορίθμων & Πολυπλοκότητας

Εαρινό Εξάμηνο 2013-2014

Εργασία Μαθήματος

Η παράδοση της εργασίας:
-είναι απαραίτητη προϋπόθεση για προβιβάσιμο βαθμό στο μάθημα.
-γίνεται ηλεκτρονικά στο *moodle* του μαθήματος (παράδοση με e-mail δεν θα γίνει αποδεκτή)
-πρέπει να γίνει *αυστηρά* μέχρι τις 6/10/2014.

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.

1 Probabilistically Checkable Proofs & Inapproximability

i. Δείξτε ότι υπάρχει μία σταθερά $\rho < 1$, τέτοια ώστε το πρόβλημα του υπολογισμού μιας ρ-προσέγγισης στο MAXCUT είναι **NP**-hard.

ii. Δείξτε ότι αν $\texttt{SAT} \in \mathbf{PCP}(r(n), 1)$, για $r(n) = o(\log n)$, τότε $\mathbf{P} = \mathbf{NP}$.
Ποιά σημαντική ένδειξη μας δίνει αυτό το αποτέλεσμα;

2 Counting & Quantum Complexity

Δείξτε ότι $co\mathbf{NQP} = \mathbf{C_{=}P}$.

3 Parameterized Complexity

Η Exponential Time Hypothesis (ETH εφεξής), μία διάσημη εικασία στην Θεωρία Πολυπλοκότητας, αναφέρει ότι δεν υπάρχει υποεκθετικός αλγόριθμος για το SAT, ή πιο αναλυτικά, ότι υπάρχει ένα $\varepsilon > 0$ τέτοιο ώστε το 3SAT δεν μπορεί να λυθεί σε χρόνο $\mathcal{O}(2^{\varepsilon n})$. Δείξτε ότι αν $\mathbf{W}[1] = \mathbf{FPT}$, τότε η ETH είναι λανθασμένη.

4 Pseudorandomness & Derandomization

Έστω $G : \{0,1\}^* \to \{0,1\}^*$ συνάρτηση υπολογίσιμη σε πολυωνυμικό χρόνο, τέτοια ώστε $|G(x)| = S(|x|)$ για κάθε $x \in \{0,1\}^*$, όπου $S : \mathbb{N} \to \mathbb{N}$ (θυμηθείτε ότι η S ονομάζεται stretch function). Η G ονομάζεται ''μη-προβλέψιμη'' αν για κάθε $B \in \mathbf{BPP}$ υπάρχει μία αμελητέα[1] συνάρτηση $\varepsilon : \mathbb{N} \to [0,1]$ τέτοια ώστε

$$\mathbf{Pr}[B(1^n, y_1, y_2, \ldots, y_{i-1}) = y_i] \leq \frac{1}{2} + \varepsilon(n)$$

δηλαδή, το να προβλέψουμε το i-οστό bit δεδομένων των $i-1$ προηγούμενων, είναι υπολογιστικά δύσκολο για κάθε πιθανοτικό αλγόριθμο πολυωνυμικού χρόνου.
Δείξτε ότι μία συνάρτηση G που είναι pseudorandom generator (με stretch function S, και ε-ψευδοτυχαία έναντι σε κάθε **BPP** adversary), είναι και μη-προβλέψιμη.

[1] Μία συνάρτηση $\varepsilon : \mathbb{N} \to [0,1]$ λέγεται αμελητέα αν $\varepsilon(n) = n^{-\omega(1)}$.

5 Expander Graphs

(*Μείωση σφάλματος* **RP** *αλγορίθμων με χρήση expanders*:) Έστω $A \in \mathbf{RP}$. Ως γνωστόν, μπορούμε να μειώσουμε την πιθανότητα σφάλματος του A επαναλαμβάνοντας τον αλγόριθμο λ φορές, το οποίο μειώνει εκθετικά την πιθανότητα λάθους, αλλά αυξάνει τα random bits που χρησιμοποιούμε κατά ένα παράγοντα λ. Θα χρησιμοποιήσουμε μια εναλλακτική μέθοδο για την μείωση του σφάλματος, που χρησιμοποιεί έναν (n, d, h)-expander που δίνεται σε explicit μορφή:

Έστω ότι ο αλγόριθμος A χρησιμοποιεί k random bits κατά την εκτέλεσή του, και έστω $G = (V, E)$ το (n, d, h)-expander γράφημα, με $V = \{0, 1\}^k$, και $h << \frac{1}{3}$ (όπου $\frac{1}{3}$ το άνω φράγμα στο σφάλμα του **RP** αλγορίθμου, όπως αναφέρεται στον κλασσικό ορισμό). Έστω ο αλγόριθμος A':

```
(1) Pick a vertex v_0 ∈ V uniformly at random.
(2) Start from it a random walk (u_0, u_1, ..., u_t) of length t.
(3) Return ⋁_{i=0}^{t} A(x, u_i).
```

1. Υπολογίστε την πιθανότητα λάθους του αλγορίθμου A' και συγκρίνετέ την με αυτή του A.
2. Υπολογίστε τον αριθμό των random bits που χρησιμοποιεί ο A' και συγκρίνετέ τον με αυτόν του A.