ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Final Exam, Topics in TCS 2016

- You are only allowed to have a handwritten A4 page written on both sides.
- Communication, calculators, cell phones, computers, etc... are not allowed.
- Your explanations should be clear, well motivated, and proofs should be complete.
- The solutions to the questions of the exam are rather short. If you end up writing a solution requiring a lot of pages then there is probably an easier solution.
- **Do not touch until the start of the exam.**

Good luck!

Name: ____________________ **N° Sciper:** ______________

Problem 1 / 25 points	Problem 2 / 25 points	Problem 3 / 25 points	Problem 4 / 25 points

Total / 100

1 (*25 pts*) **Basics.** In this problem, you should answer whether the following 10 statements are true or false.

- We have a proof that $\mathbf{BPP} \subseteq \mathbf{NP}$. True or False? False
- We have a proof that $\mathbf{BPP} \subseteq \mathbf{BQP}$. True or False? True
- We have a proof that $\mathbf{BPP} \subseteq \mathbf{P}_{/\mathbf{poly}}$. True or False? True
- We have a proof that $\mathbf{NP} \subseteq \mathbf{BQP}$. True or False? False
- We have a proof that $\mathbf{P}_{/\mathbf{poly}} \subseteq \mathbf{NP}$. True or False? False
- We have a proof that $\mathbf{IP} \subseteq \mathbf{EXP}$. True or False? True
- We have a proof that $\mathbf{PH} \subseteq \mathbf{PSPACE}$. True or False? True
- We have a proof that $\mathbf{PCP}(O(1), \text{poly}(n)) = \mathbf{P}$. True or False? False
- We have a proof that $\mathbf{PCP}(\log n, O(1)) = \mathbf{NP}$. True or False? True
- If $\mathbf{NP} \neq \mathbf{coNP}$, then $\mathbf{P}^{\mathbf{NP}} \neq \mathbf{NP}$. True or False? True

The correction is as follows: 10 correct answers give 25 points, 9 correct answers give 22 points, 8 correct answers give 17 points, 7 correct answers give 10 points, 6 correct answers give 5 points, 5 or less correct answers give 0 points.

2 *(25 pts)* **The Polynomial Hierarchy.** Show that if **PH** = **PSPACE** then the polynomial hierarchy collapses to some level.

In this problem you are allowed to use (if you wish) the following statement proved in class: for every $i \geq 1$, if $\Sigma_i^p = \Pi_i^p$ then $\mathbf{PH} = \Sigma_i^p$. All other statements should be proved.

(*Hint:* use the fact that **PSPACE** has complete languages.)

Solution:

- Suppose that **PH** = **PSPACE**.
- Let L be a **PSPACE** complete problem (here we use the hint).
- Then, with our assumption, L is also complete for **PH**.
- Now let i be such that $L \in \Sigma_i^p$ (such an i exists since $L \in \mathbf{PH}$). In other words there exists a polytime TM M such that

$$x \in L \Leftrightarrow \exists u_1 \forall u_2 \ldots Q_i u_i M(x, u_1, u_2, \ldots, u_i) = 1.$$

We now prove that in this case $\mathbf{PH} \subseteq \Sigma_i^p$, i.e., the polynomial hierarchy collapses to its i:th level.

- Consider any $L' \in \mathbf{PH}$.
- As L is a complete problem for **PH** we have that any $L' \in \mathbf{PH}$ has a polynomial time reduction to L. Let M' be the TM representing this reduction, i.e., $x' \in L' \Leftrightarrow M'(x') = x \in L$.
- Using this reduction together with that $L \in \Sigma_i^p$, we have

$$x' \in L' \Leftrightarrow \exists u_1 \forall u_2 \ldots Q_i u_i M(M'(x'), u_1, u_2, \ldots, u_i) = 1.$$

- Notice that this implies that $L' \in \Sigma_i^p$ since both M and M' run in polynomial time the TM on the RHS runs in polytime.

3 *(25 pts)* **Circuits.** Prove the following statement:

> Let $\epsilon > 0$ and $d(n) = (1-\epsilon) \cdot n$. Then for n large enough there exists an n-ary function $f : \{0,1\}^n \to \{0,1\}$ not computable by circuits of depth at most $d(n)$.

In this problem, we only allow gates of fan-in 2 (or 1 if it is a NOT gate).

(*Hint:* recall that most functions f require circuits of large size. In particular, you are allowed to use the statement proved in class about the circuit size of most functions.)

Solution:

- We know from class that there exists a function $f : \{0,1\}^n \to \{0,1\}$ that requires $\Omega(2^n/n)$ gates.
- Now how many gates can a circuit of depth $d(n)$ have?
- Well there is one gate that produces this input. The fan-in to this gate is at most two. So there are at most 2 gates connecting to the output gate. Continuing this argument there is at most 4 gates connecting to these 2 gates and so on.
- In total a circuit of depth $d(n)$ can have at most

$$\sum_{i=0}^{d(n)} 2^i = 2^{d(n)+1} - 1 \text{ gates.}$$

- As $2^{(1-\epsilon)n+1}$ is much smaller than $2^n/n^2$ for large enough n the statement of the exercise follows.

4 *(25 pts)* **Hardness and PCPs.** Recall that in the Vertex Cover problem, you are given a graph $G = (V, E)$, and the goal is to find the minimum subset $S \subseteq V$ of vertices such that each edge $e \in E$ has at least one endpoint in S. We saw in problem set IV that, using Håstad's 3-bit PCP verifier, we can prove that it is NP-hard to approximate the Vertex Cover problem within a factor of $7/6 - \varepsilon$ for any $\varepsilon > 0$. In particular, Håstad's PCP verifier queries 3 bits of the proof and checks whether a certain predicate is satisfied, while having a completeness of $1 - \varepsilon$ and soundness $1/2 + \epsilon$.

In this problem, you are asked to prove that it is NP-hard to approximate vertex cover within $2 - \varepsilon$ for any $\varepsilon > 0$, *assuming*[1] the following PCP verifier $\widetilde{V}$ exists for SAT:

> For every $\varepsilon > 0$, there exists a large enough **constant** k such that $\widetilde{V}$ uses $O(\log n)$ random bits to compute k positions in the proof π, say $i_1, \ldots, i_k$, and accepts iff $C(\pi(i_1), \ldots, \pi(i_k)) = 1$, where C is a fixed predicate of the verifier $\widetilde{V}$ that has exactly **two satisfying assignments**. Formally, C is a predicate $C : \{0,1\}^k \mapsto \{0,1\}$ such that there exist only **two** partial assignments $z_1, z_2 \in \{0,1\}^k$ (out of the 2^k possible ones) such that $C(z_1) = C(z_2) = 1$ and $C(z) = 0$ for all $z \in \{0,1\}^k \setminus \{z_1, z_2\}$. The verifier $\widetilde{V}$ has completeness $1 - \varepsilon$ and soundness ϵ. In other words:
>
> – if φ is a satisfiable SAT instance then there is a proof π that makes the verifier accept with probability at least $1 - \varepsilon$.
>
> – if φ is not a satisfiable SAT instance then for any proof π, the verifier accepts with probability at most ε.

Your task in this problem is to use the above described verifier $\widetilde{V}$ to prove that it is NP-hard to approximate Vertex Cover within a factor of $2 - \varepsilon$, for any $\varepsilon > 0$.

Solution:

- Suppose the number of random bits queried by $\widetilde{V}$ is $c \log n$.
- We know construct the FGLSS graph with a vertex for each accepting configuration. That is for each random string r we will have exactly two vertices corresponding to the two accepting configurations. The total number of vertices is thus $N := 2^{c \log n} = 2 \cdot n^c$.
- The edges are the same as in the homework: two vertices are adjacent if they have conflicting opinions/assignments to the same bit in the proof.
- Now in the YES/Completeness case there is a proof π that makes $\widetilde{V}$ accept with probability at least $1 - \varepsilon$. If we take all the vertices corresponding to that proof we get a set of size at least $n^c(1 - \varepsilon)$ and its complement is a vertex cover of size at most $(1 + \varepsilon)n^c$.
- Now in the NO/Soundness case any proof makes $\widetilde{V}$ accept with probability at most ε. By the same analysis as in class, this implies that the FGLSS graph has an independent set of size at most εn^c. In other words, any vertex cover has size at least $(2 - \varepsilon)n^c$.
- The inapproximability of $\frac{2-\varepsilon}{1+\varepsilon} \geq 2 - \varepsilon'$ for any $\varepsilon' > 0$ follows.

[1] This verifier is only known to exist under a stronger complexity theoretic assumption, known as the Unique Games Conjecture.