COS 522 Complexity - Spring 2006 - Final Take Home Exam

- Read these instructions carefully *before* starting to work on the exam. If any of them are not clear, please email me before you start to work on the exam.

- **Schedule:** You can work on this exam in a period of 48 hours of your choice between May 1^{st} to **May 15^{th} 1:30pm**. The exam needs to be submitted to **Mitra Kelly (Room 323)** by May 15^{th} 1:30 pm. *This is a strict deadline.* You may submit the exam earlier. If you typed up your exam, I would appreciate it if you also email me a copy of it at the same time. In any case, please email me when you have submitted the exam.

- **Restrictions , honor code:** You should work on the exam alone. You can use your notes from the class, the homework exercises and their solutions, the textbook and the handouts I gave in class. You can also use any personal summaries and notes of the material that you prepare before starting to work on the exam. *You should not use any other material while solving this exam.* You should write and sign the honor pledge on your submitted exam (the pledge is "I pledge my honor that I did not violate the honor code during this exam and followed all instructions").

- **Writing:** You should answer all questions *fully*, *clearly* and *precisely*. When describing an algorithm or protocol, state clearly what are the inputs, operation, outputs, and running time. When writing a proof, provide clear statements of the theorem you are proving and any intermediate lemmas or claims. I recommend that you first write a draft solution of all questions before writing (or preferably, typing) up your final submitted exam.

- **Partial solutions:** If there is a question you can not solve fully, but you can solve a partial/relaxed version or a special case, then please state clearly what is the special case that you can solve, and the solution for this case. You will be given partial credit for such solutions, as long as I feel that this special case captures a significant part of the question's spirit.

- **Quoting results:** You can quote without proof theorems that were proven in class. You can also use without proofs standard mathematical tools such as Chernoff bounds, and concepts from linear algebra (inner product, eigenvalues etc.). However, you should quote the results precisely, and give a reference to the date and number the result was proven, or to the place in the textbook where the result is stated. When solving a question, you can use the results of a previous question as given, even if you did not manage to solve it.

- **Points:** The exam has 6 questions, with each worth 20 points (total of 120 points).

- **Clarifications:** I have made an effort to make the questions as clear and unambiguous as possible. In case any clarifications are needed, I will try to be always available by email. You can also email me with your number and good times to call, and I will call you back. If you need me more urgently, you can call me at my cell phone 917-674-6110 between 11am and 10pm eastern time. If there are any unresolved doubts, please write your confusion as part of the answer and maybe you will get partial credit.

Turn the page only when you are ready to start working on the exam.

This exam has a total of 6 questions, each worth 20 points, summing up to 120 points.

Question 1. Prove that if $\mathbf{NP} = \mathbf{P}$ then there exists a function f in $\mathbf{E} = \mathbf{DTIME}(2^{O(n)})$ and a constant $\epsilon > 0$ such that f can not be computed by circuits of size $2^{\epsilon n}$.

Question 2. We say that a language $L \subseteq \{0,1\}^*$ is *sparse* if there exists a polynomial $p : \mathbb{N} \to \mathbb{N}$ such that for every n, $|L \cap \{0,1\}^n| \leq p(n)$. We say that L is $\mathbf{NP}$-*complete* if there exists a polynomial-time computable function f such that for every 3CNF formula φ, $\varphi \in \mathsf{3SAT} \iff f(\varphi) \in L$.

1. Prove that if a sparse language L is $\mathbf{NP}$-complete then the polynomial hierarchy collapses.
2. Prove that if a sparse language L is $\mathbf{NP}$-complete then $\mathbf{NP} = \mathbf{P}$. (Hint: think of downward self-reducibility and dynamic programming.)

Question 3. Let $f = \{f_n\} \in \mathbf{AC^0}$. Prove that f can be 90%-approximated by a family of circuits $\{C_n\}$ where each circuit C_n is of polynomial-size, depth three, and consists of a single unbounded fanin parity gate at the top, and polynomially many $\wedge$ and $\vee$ gates, each with polylogarithmic fanin. (We assume that $\neg$ gates are at the bottom, or equivalently the inputs to the circuit are $x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n$, for simplicity you may assume the circuit also gets the constants 0 and 1 as additional inputs.) An n-input circuit C 90%-approximates a function $f : \{0,1\}^n \to \{0,1\}$ if for a random $x \leftarrow_{\mathrm{R}} \{0,1\}^n$, $C(x) = f(x)$ with probability ≥ 0.9.

Question 4. Throughout this course, we often used the fact that for every $x \in \{0,1\}^n$ with $x \neq 0^n$, $\Pr_{r \leftarrow_{\mathrm{R}} \{0,1\}^n}[\langle x, r\rangle \pmod 2 = 1] = 1/2$. We now ask whether we can choose r using fewer than n random bits.

1. Prove that for every $\epsilon > 0$ there exists a set $S \subseteq \{0,1\}^n$ of size $\mathrm{poly}(n, 1/\epsilon)$ such that

$$\tfrac{1}{2} - \epsilon < \Pr_{r \leftarrow_{\mathrm{R}} S}[\langle x, r\rangle \pmod 2 = 1] < \tfrac{1}{2} + \epsilon \tag{1}$$

2. Let S be a set satisfying (1) for $\epsilon \leq 1/10$ and let A be an $|S| \times n$ matrix whose rows are elements of S. Prove that the function $ECC : \{0,1\}^n \to \{0,1\}^{|S|}$ defined as follows: $ECC(x) = Ax$ is an *error correcting code* with distance at least 1/4. That is, for any $x \neq x' \in \{0,1\}^n$ the fractional Hamming distance of $ECC(x)$ and $ECC(x')$ is at least 1/4.
3. Show an explicit construction of a set S of size $\mathrm{poly}(n)$ that satisfies (1) for $\epsilon = 1/10$. That is, show a polynomial-time algorithm that on input 1^n outputs the list of elements of such a set S.

Question 5. Call a set S satisfying (1) above "ϵ-nice".

1. For a set $S \subseteq \{0,1\}^n$, let S' be the corresponding subset of $\{\pm 1\}^n$ (where we identify $\{0,1\}$ with $\{\pm 1\}$ in the usual way of $0 \mapsto +1$, $1 \mapsto -1$). Consider the function $f : \{\pm 1\}^n \to \mathbb{R}$ defined as follows: for $x \in \{\pm 1\}^n$, $f(x) = 1$ if $x \in S'$ and $f(x) = 0$ otherwise. As in class, for $\alpha \subseteq [n]$ and $x \in \{\pm 1\}^n$ let $\chi_\alpha(x) = \prod_{i \in \alpha} x_i$ and $\hat{f}(\alpha) = \mathbb{E}_{x \leftarrow_{\mathrm{R}} \{\pm 1\}^n}[f(x)\chi_\alpha(x)]$.

   Let $\mu = \frac{|S|}{2^n}$. Prove that $\hat{f}(\emptyset) = \mu$ and that if S is ϵ-nice then for $\alpha \neq \emptyset$, $|\hat{f}(\alpha)| \leq 2\mu\epsilon$.

2. Let S be an ϵ-nice set. Define a graph G with 2^n vertices and degree $|S|$ as follows: we put an edge between $x, y \in \{0,1\}^n$ if $x \oplus y \in S$. Recall that $\lambda(G)$ denotes the absolute value of the second-largest eigenvalue of the normalized adjacency matrix of G. Prove that if S is ϵ-nice then $\lambda(G) \leq 2\epsilon$. (Hint: the family of 2^n eigenvectors for this matrix is quite natural.)

Question 6. We define a *non-deterministic* circuit to be a Boolean circuit C that takes two inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^m$ where we define that C accepts the input x iff $\exists y \in \{0,1\}^n$ such that $C(x,y) = 1$ (i.e., we think of the second input as a witness/certificate for the first input). Recall the language GNI containing pairs of adjacency matrices of graphs that are *not* isomorphic. Prove that GNI can be decided by a polynomial-sized family $\{C_n\}$ of non-deterministic circuits (i.e., for every $x \in \{0,1\}^n$, C_n accepts x iff $x \in \mathsf{GNI}$.) Note that it's not known whether or not $\mathsf{GNI} \in \mathbf{NP}$.