Qualifying Examination

Theoretical Computer Science

Thursday, March 6, 2014

Part II: Automata and Complexity

Name	

Problem	Maximum Points	Points Earned	Grader
1	25		
2	25		
3	25		
4	25		
Total	100		

Instructions:

1. This is a closed book exam.
2. The exam is from 9am–5pm and has four problems of 25 points each. Read all the problems carefully to see the order in which you want to tackle them.
3. Write clearly and concisely. You may appeal to some standard algorithms/facts from text books unless the problem explicitly asks for a proof of that fact or the details of that algorithm.
4. If you cannot solve a problem, to get partial credit write down your main idea/approach in a clear and concise way. For example you can obtain a solution assuming a clearly stated lemma that you believe should be true but cannot prove during the exam. However, please do not write down a laundry list of half baked ideas just to get partial credit.

May the force be with you.

Problem 1: Thanks to its breakthrough on black-box quantum computing, Q-Wave Inc. has built a machine that can solve large instances of NP-complete problems. Q-Wave makes money through a service by which one can submit an NP problem, in the form of a Boolean circuit C, and then the next day, for a fee of \$100,000 dollars, one gets back an input x such that $C(x) = 1$ if such an input exists. (Or the assurance that no such x exists, otherwise.)

You set up a reselling business that, for the same service, charges only \$2,000 dollars per circuit, but you only guarantee to give back the answer within three weeks. You expect to get about 100 requests per day, and to make a profit. How is it possible?

Technically, prove the following fact: suppose you are given m circuits $C_1, \cdots, C_m$ and for each of them, you want to find an x_i such that $C_i(x_i) = 1$, if such an x_i exists. Show that you can solve this problem in time polynomial in the sum of the sizes of the circuits provided that you are given access $\lceil \log_2 m + 1 \rceil + 1$ times to an "oracle" that given a circuit C finds an x such that $C(x) = 1$ if such an x exists, or that tell you that no such x exists otherwise. (For example, given 1023 circuits, you can solve the circuit sat search problem for all of them if you are given access 11 times to an oracle for the circuit sat search problem.)

Problem 2: We will say that a string $w \in \Sigma^*$ is idempotent for $L \subseteq \Sigma^*$ if for every $u, v \in \Sigma^*$

$$uwv \in L \Leftrightarrow uwwv \in L$$

Prove that for any regular language $L \subseteq \Sigma^*$, there is a natural number n such that w^n is idempotent for L, for any $w \in \Sigma^*$. (Here w^n denotes the concatenation of n copies of w.)

Problem 3: Recall that a language A is said to be in *uniform* $\mathbf{NC}^i$ iff there is a family of circuits $\{C_n\}_{n \in Z}$ using $\neg, \wedge, \vee$ gates with fan-in at most 2 such that (a) there is a logspace machine that given input 1^n outputs circuit C_n; (b) C_n has size (number of gates) at most polynomial in n, and depth $(\log n)^i$; and (c) for every $x \in \{0,1\}^n$, $x \in A$ iff $C_n(x) = 1$.

Prove that *uniform* $\mathbf{NC}^1 \subseteq \mathbf{L} \subseteq \mathbf{NL} \subseteq$ *uniform* $\mathbf{NC}^2$.

Problem 4: Consider a function $f : \{0,1\}^n \times \{0,1\}^n \to \{+1, -1\}$. We associate a $2^n \times 2^n$ matrix M with f, which has its rows and columns indexed by n-bit strings and has entries ± 1, defined by $M_{x,y} = f(x, y)$.

A monochromatic *tile* of M is a set $A \times B$, with $A, B \subseteq \{0,1\}^n$ such that $\forall (x, y) \in A \times B$, $f(x, y)$ takes the same value. A monochromatic *tiling* of M is a

partition of $\{0,1\}^n \times \{0,1\}^n$ into monochromatic tiles of M. A very useful measure for bounding the communication complexity of f is $\chi(f)$ defined as the minimum number of tiles in any monochromatic tiling of f.

Another very useful measure of complexity of f is its *discrepancy*, $\mathrm{Disc}(f)$ defined as follows.

$$\mathrm{Disc}(f) = \max_{A,B \subseteq \{0,1\}^n} \Delta(A \times B) \quad \text{where}$$
$$\Delta(A \times B) = \frac{1}{2^{2n}} \left| \sum_{x \in A, y \in B} M_{x,y} \right|.$$

1. Show that $\chi(f) \geq \frac{1}{\mathrm{Disc}(f)}$.

2. Suppose f is a *symmetric* function, that is $f(x,y) = f(y,x)$ for all x, y. Then the eigenvalues of M are real. Let λ be the largest absolute value of an eigenvalue of M. Show that for all $A, B \subseteq \{0,1\}^n$,

$$\Delta(A \times B) \leq \frac{1}{2^{2n}} \lambda \sqrt{|A \times B|}.$$

   You may use the fact that for all vectors $v, w \in \mathbb{R}^{2^n}$, $v^T M w \leq \lambda \langle v, w \rangle$.

3. Use the preceding part to show that if f is the inner-product function over $GF(2)^n$ (using ± 1 outputs), i.e., $f(x,y) = (-1)^{\langle x,y \rangle}$, then $\chi(f) \geq 2^{n/2}$. You may use the fact that for this f, $\lambda = 2^{n/2}$.