COMP 531: Advanced Theory of Computation (Winter 2014)

Assignment 5

Due April 11th

Instructions

Follow these instructions closely.

You will benefit most if you seriously try solving each problem yourself. You may work with each other but you must write up your own solutions. For each question, you should clearly acknowledge the people you have worked with. You are not allowed to use any resources that contain the solution to an assignment question. However, we value honesty above all. You will get full marks if you happen to find the solution to a question and you write your own solution, **as long as you properly acknowledge your source**. Failure to acknowledge your source can result in 0 points.

Clarity and conciseness of your solutions are as important as correctness. It is important to learn how to write your ideas and solutions clearly and rigorously. You will lose marks for correct solutions that are poorly explained/presented. When writing your solutions, assume that your audience is your class mates rather than the instructor of the course. The high level ideas and an overview of your argument should be presented before any technical details, and all non-trivial claims have to be proven.

If you do not know how to solve a problem, do not answer it. This will earn you 20% of the points. Do not make yourself believe in a wrong proof, this is bad for you. **And definitely do not try to sell it!** If you don't know how to solve a problem but you have some non-trivial ideas, write them down. If you have a solution with gaps, write your argument and clearly indicate the gaps.

Submit your assignments in class or send a copy to `aada@cs.mcgill.ca` before midnight of the due date.

Questions

1. In Assignment 4, you were asked to answer two of the following questions: Question 1, Question 2, and Question 4. This question asks you to answer the question that you left out.

2. Let H be a universal family of hash functions from n bits to m bits. Let $U \subset \{0,1\}^n$ be a set of elements to be hashed.

   (a) Let $a = |U|/2^m$. Prove that $(a - a^2/2) \le \Pr_{h,t}[\exists x \in U \text{ s.t. } h(x) = t] \le a$.

   (b) Suppose $2^{m-2} \le |U| \le 2^{m-1}$. Call an element x of U isolated by h, if $\forall y \in U$ with $y \neq x$, $h(x) \neq h(y)$. Show that the expected number of elements isolated by a random $h \in H$ is at least $|U|/2$. Show that

   $$\Pr_{h,t}[\exists \text{ unique } x \in U \text{ s.t. } h(x) = t] \ge 1/8.$$

3. Let M be a circuit consisting of a MAJORITY gate at the output that is being fed by sub-circuits $c_1, c_2, \ldots, c_n$ each taking up to n inputs. Thus M outputs 1 on input $x \in \{0,1\}^n$ if and only if $\sum_{i=1}^{s} c_i(x) \ge s/2$. Let f be the boolean function that is computed by M. Show that if $\mathrm{Cor}_U(f, c_i) \le \epsilon$ for all i, then $s \ge 1/\epsilon$. Here U denotes the uniform distribution, and correlation has been defined both in class and Assignment 3.

   This statement gives us a tool to prove lower bounds for circuits that have a MAJORITY gate at the output. If f is a function that has very small (e.g. exponentially small) correlation with all the c_i's, then the circuit as described above must have very large size (e.g. exponentially large) in order to compute f.