

Complexity Homework 5

Released: April 30, 2007

Due: May 10, 2007

No collaboration is allowed in this homework. However, this is a relatively short and easy homework.

Problem 1:

For binary strings of equal length, define a partial order \leq as follows: $x \leq y$ iff $x_i = 1 \implies y_i = 1$ for all positions i .

A boolean *function* $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is called *monotonic* if $x \leq y \implies f(x) \leq f(y)$. That is, if $f(x) = 1$, then changing any number of bits of x from 0 to 1 (i.e., “increasing” x) will not change (i.e., “decrease”) the value of the function to 0.

A boolean *circuit* is called *monotone* if it consists only of AND and OR gates.

Show that a boolean function is monotonic iff it is computed by a monotone circuit.

Problem 2:

Recall the definition of elusiveness (Lecture 21). Give an adversary argument to show that a function defined by a monotonic tree circuit¹ is elusive. Note that the adversary strategy should specify how to answer a queried bit (as 0 or as 1) based on the previous queries and answers.

Problem 3:

Consider boolean functions on n -bit inputs: i.e., functions of the form $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Let us call such a function t -varying if (i) for any setting of any t bits of the inputs, there are two ways to set the remaining $n - t$ bits so that the output is 0 and 1 respectively, but (ii) there is a way to set $t + 1$ bits such that it fixes the output value.

1. Give an example of an *elusive* function which is 0-varying, and another elusive function which is $(n - 1)$ -varying. Which are the $(n - 1)$ -varying functions? Prove.
2. Show that most boolean functions on n -bit inputs are t -varying with $t \geq n - n^\epsilon$ for a constant $0 < \epsilon < 1$. You may follow the steps below.
 - (a) Consider some k positions out of n positions, and fix the bit values on the other $n - k$ positions to some values. What is the probability that a random function remains constant over all inputs which are consistent with the fixed bit values?
 - (b) Give a bound on the total number of ways the above described restriction (choosing $n - k$ positions and fixing bit values on those positions) can be done.
 - (c) Use the union bound to derive a bound on the probability that a random function is t -varying for some $t < n - k$. Consider $k = n^\epsilon$.

Problem 4:

Show that an n -variate polynomial over $\text{GF}(q)$ (the finite field of q elements) of degree at most d evaluates to 0 on at most d/q fraction of the possible q^n assignments of values to the variables. You can use the fact that this holds for $n = 1$ (i.e., a degree d *univariate* polynomial has at most d roots).

Problem 5:

(This is one direction of Problem 12.10 from the textbook.)

Suppose we are given a boolean circuit of fan-in 2, and depth d , that computes a boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Consider the following communication problem related to f . Alice gets an input x such that $f(x) = 0$ and Bob gets an input y such that $f(y) = 1$, and they must both output i such that $x_i \neq y_i$. (Clearly $x \neq y$ and therefore there must be at least one position i such that $x_i \neq y_i$.) Give a protocol for this

¹See Lecture 21. For an example see the AND-OR function of Example 11.6 from the textbook.

task in which the total number of bits exchanged is at most the depth of the circuit d . Prove the correctness of the protocol.

(Hint: Consider Alice and Bob traversing the circuit from its output gate to one of its input gates, maintaining the invariant that they disagree on the output of the current gate. At each step, at most one party sends a single bit.)

Extra credit: Argue the converse, that any protocol for the above communication problem can be turned into a circuit of depth equal to the maximum number of bits exchanged in the protocol. *(Hint: the transformation indeed takes the protocol built above and gives the original circuit.)*