6.841: Advanced Complexity Theory Fall 2012

Problem Set 2 – Circuit Lower Bounds

Prof. Dana Moshkovitz/TA: Henry Yuen *Due Date: October 4, 2012*

Turn in your solution to each problem on a separate piece of paper. Mark the top of each sheet with the following: (1) your name, (2) the question number, (3) the names of any people you worked with on the problem. We encourage you to spend time on each problem individually before collaborating!

Problem 1 – Circuit lower bound for MAJORITY

Define the function $\mathrm{MAJ}(x) = 1$ iff $|x| \geq n/2$, where $|x|$ denotes the number of 1s in the n-bit string x.

Prove that any circuit of constant depth d computing the function MAJ requires size $\exp(\Omega(n^{2^{-d}}))$. Hint: Use the fact that depth d circuits computing PARITY require size $\exp(\Omega(n^{2^{-d}}))$.

Problem 2 – Some combinatorial scaffolding

In the next two problems, we'll explore some more limitations of small-depth circuits. But first, we need to set up some useful combinatorial lemmas.

(a) *The Flower Lemma.* Let $\mathcal{U}$ be a universe of elements. A family of sets $S_1, \ldots, S_t \subset \mathcal{U}$ form a *flower* with k petals and with *core* Y iff the following properties holds:

1. $Y \subseteq S_i$ for all i;
2. If a set $T \subseteq \mathcal{U}$ intersects each $S_i - Y$ in at least one element, then $|T| \geq k$. Such Ts are called *blocking sets* of the flower.

Every sunflower with k petals is a flower with k petals, but the converse is not necessarily true[1].

Prove the following variant of the Sunflower Lemma: let $\mathcal{F}$ be a family of sets each of cardinality ℓ. If $|\mathcal{F}| > (k-1)^\ell$ then $\mathcal{F}$ contains a flower with k petals.

(b) We say $x \in \{0,1\}^n$ is a k-limit for $A \subseteq \{0,1\}^n$ iff for every subset $S \subset \{1, \ldots, n\}$, $|S| = k$, there exists $u \in A$ such that $x \leq u$ ($x_i \leq u_i$ for all i), and furthermore for all $j \in S$, $x_j = u_j$.

Let $|x|$ denote the number of 1s in x. Let A be a set of size greater than k^s, where for all $a \in A$, $|a| = s$. Let $B = \{x \in \{0,1\}^n \mid |x| \leq s-1\}$.

Show that there exists $v \in B$ that is a k-limit for A. Hint: Use the Flower Lemma from the previous part.

[1] An example would be $\mathcal{F} = \{\{1,2\},\{2,3\},\{3,4\},\{4,5\},\{5,1\}\}$. It is easy to see that this is a flower with 3 petals and an empty core, because every blocking set of $\mathcal{F}$ must have 3 elements; but $\mathcal{F}$ is not a sunflower with 3 petals, nor does it contain a sunflower with 3 petals.

Problem 3 – Formula size lower bounds on threshold functions

We're going to put to use the combinatorial machinery you built in the last problem to show that threshold functions require exponential sized depth 3 formulas.

The *s-threshold function* $T_s : \{0,1\}^n \to \{0,1\}$ is defined as $T_s(x) = 1$ iff $|x| \geq s$.

(a) Show that T_s can be computed by a depth 2 monotone circuit of size $O(\binom{n}{s})$.

Could one do substantially better if we allow more depth and allow negations? It turns out that we can't, if we add only one more layer to our circuit. We're going to specifically analyze the size of OR-AND-OR formulas required to compute T_s. An OR-AND-OR formula, as its name suggests, is a depth 3 circuit where the top gate is an OR gate, the second layer consists of ANDs, and the third layer consists of ORs. The inputs may be repeated and have negations.

Alternatively, an OR-AND-OR formula F is one where $F = F_1 \vee F_2 \vee \cdots \vee F_t$, where each F_i is a CNF formula – i.e., an AND of clauses that are ORs of literals. The bottom fan-in of a formula is the maximum number of literals in each clause.

Let $F = F_1 \vee F_2 \vee \cdots \vee F_t$ be an OR-AND-OR formula with bottom fan-in k. Suppose that F rejects all input strings with fewer than s 1's. We'll show that F cannot accept more than tk^s strings with exactly s 1's. For sake of contradiction, let's assume that F does accept more than tk^s strings of weight s (where the weight of x means $|x|$).

(b) Show that there must be a AND-OR subformula F_i that accepts a set A of strings that have weight exactly s, and $|A| > k^s$.

(c) Let B be the set of strings with weight at most $s - 1$. Show that there exists $\alpha \in B$ that is a k-limit for A.

(d) Show that the subformula F_i associated with A must accept α, and derive a contradiction.

(e) What lower bound do we get on the size of OR-AND-OR formulas (with bottom fan-in k) that compute T_s?

Problem 4 – Complexity of Problem Setting

How many hours have you spent on this problem set and on Problem Set 1?