MATH 642:582–Fall, 2003

Assignment 6 (OPTIONAL)–Due December 12 (Version: December 4, 2003)

1. Jukna 8.5

2. In this problem a "depth k circuit" over variables $x_1, \ldots, x_n$ is an acyclic digraph satisfying:

   - The vertices can be partitioned into layers $L_0, L_1, \ldots, L_k$ so that each edge goes from L_i to L_{i-1} for some i.
   - L_0 consists of a single vertex called the output node.
   - L_k consists of $2n$ vertices of in-degree 0, labeled $x_1, \ldots, x_n, \neg x_1, \ldots, \neg x_n$ (These are the input vertices).
   - Each noninput vertex (or "gate") at even distance from the root is labeled by $\wedge$ and each at odd distance from the root is labeled by $\vee$. (Thus the root is labeled $\wedge$.)

   Such a circuit computes a boolean function in the obvious way. The size of a circuit is the number of gates. The *bottom fan-in* of the circuit is the maximum in-degree of gates at level $k-1$.

   Let $P(n,k)$ be the size of the smallest circuit computing the parity (sum mod 2) function on n variables. The purpose of this problem is to prove the following theorem of HÅstad: $P(n,k) \geq 2^{c_0(c_1 n)^{1/k-1}}$ for some positive constants c_0 and c_1.

   (a) Prove that $P(n,2) = 2^{n-1}$.

   (b) Prove the following Lemma: Let $n = m^{k-1}$ and $s, t \leq m/10$. Let f be an n-variate boolean function. Suppose f can be computed by a circuit C having depth k, bottom fan-in at most t and size at most 2^s. Then there is a restriction ρ of f leaving m^{k-2} variables unfixed such that the restriction $f\lceil_\rho$ can be computed by a circuit of depth $k-1$, size at most 2^s and bottom fan-in at most s. (Hint: Use the switching lemma).

   (c) Prove the theorem.

3. (a) Let $x_1, \ldots, x_n$ be real variables and for $J \subseteq \{1, \ldots, n\}$ write x^J for $\prod_{j \in J} x_j$. Let $f : \{0,1\}^n \longrightarrow \{0,1\}$ be a boolean function. Prove that there are unique real numbers $(a_J : J \subseteq [n])$ such that the real polynomial $\sum_j a_j x_J$ agrees with f on $\{0,1\}^n$.

   (b) Define the degree of a boolean function f, $deg(f)$, to be the degree of the representing polynomial found in the previous section. Prove that the decision tree complexity $DT(f)$ is at least $deg(f)$.

   (c) An n-variate function f is *evasive* if $DT(f) = n$, i.e., is a bad as possible. Prove that a non-evasive function must satisfy the condition that the number of inputs in $f^{-1}(1)$ having an even number of 1's is equal to the number of inputs in f^{-1} having an odd number of 1's.

4. If f is an n variate boolean function and σ is a permutation of $[n]$ we write f_σ for the boolean function defined by $f_\sigma(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. The automorphism group of f is the set of σ such that $f = f_\sigma$ (which is obviously a group). f is weakly symmetric if the automorphism group is transitive, which means that for any i, j in $[n]$ there is an automorphism σ mapping i to j.

   Prove the following theorem of Rivest and Vuillemin (1976). Suppose $n = p^k$ for some prime p and integer k. Suppose that f is a boolean function on n variables, f is weakly symmetric and that $f(0^n) \neq f(1^n)$. Then f is evasive(!) (Hint: Let G be the automorphism group of f and let $\mathcal{P}$ be the partition of $\{0,1\}^n$ into orbits under the action of G. Prove that there are exactly two orbits whose size is not divisible by p. Then use the previous problem.)