CSE 532 Spring 2004
Computational Complexity Essentials
Exercises #1

Problems:

1. Show that if $\mathsf{NP} \subseteq \mathsf{TIME}(n^{\log n})$ then $\Sigma_k\mathsf{P} \subseteq \mathsf{TIME}(n^{\log^k n})$.

2. In this problem you will prove Cobham's theorem regarding

$$\text{PALINDROME} = \{x \in \{0,1\}^* \mid x = x^R\}.$$

   For a 1-tape Turing Machine M with state set Q and tape cell i of M define the *crossing sequence* of M at on input x as the ordered sequence of states $\sigma_i \in Q^* \cup Q^\infty$ consisting of the states that M is in as it passes the boundary between cell i and cell $i+1$. Note that the directions that the read head of M moves as it crosses this boundary alternates R and L, beginning with R since M starts at the left end of the tape. Consider the behavior of a 1-tape TM M for PALINDROME that takes time $T(n)$ on inputs of the form $\{y0^{2n}y^R \ : \ n = |y|\}$. Suppose that M that (without loss of generality) M ends its computation at the right end of the input, i.e. cell $4n+1$.

   (a) Show that if M takes time at most $T(n)$ on input $y0^{2n}y^R$ then the average crossing sequence $|\sigma_i| = |\sigma_i^y|$ for $i \in [n, 3n]$ is $O(T(n)/n)$.

   (b) Show that there is some $i \in [n, 3n]$ such that $|\sigma_i^y|$ is $O(T(n)/n)$ for all y in a large subset of $\{0,1\}^n$.

   (c) Use this to show that if $T(n) = o(n^2)$ then M will accept some input of the form $y0^{2n}x^R$ for $|x| = |y| = n$ and $x \neq y$.

3. In this problem you will derive Lupanov's bound on the worst-case size required to compute any Boolean function on n bits. One of the keys is to represent functions as polynomials modulo 2. Thus every function $f : \{0,1\}^n \to \{0,1\}$ can be written as a polynomial $\sum_{\alpha \in S} \prod_{i=1}^n x_i^{\alpha_i}$ in $\mathbb{F}_2$ for some $S \subseteq \{0,1\}^n$. This naturally leads to expressions of functions in terms of the basis $\Omega = \{1, \oplus, \wedge\}$. Do the following first in terms of that basis and then adjust the size bounds for the final circuit in converting back to the De Morgan basis $\{\neg, \vee, \wedge\}$.

   (a) One can compute many functions in a single circuit by designating more than one node as an output node. Prove that for any integer p and every collection of $\{f_1, ..., f_t\}$ functions with $f_i : \{0,1\}^m \to \{0,1\}$ can be simultaneously computed using size $2^m + \lceil 2^m/p \rceil 2^p + t \cdot \lceil 2^m/p \rceil$. Do this by computing all possible monomials and suitably grouping their sums.

   (b) For a single function $f : \{0,1\}^n \to \{0,1\}$ represented as a polynomial over $\mathbb{F}_2$, group the monomials based on the common form of the last $n - \sqrt{n}$ variables and apply the construction from part (a) with $m = \sqrt{n}$ and suitable values of t and p to the functions involving the first m variables. Optimize the choice of p to obtain the best size bounds and analyze the resulting complexity as a function of n of the form $2^n/n + \theta_n$ where θ_n is $o(2^n/n)$.