Complexity Theory (Winter 2016/17) **Problem Set #3 (Due 09.01.2017)**

Problem 3.1. Show $APSPACE = EXP$.

Problem 3.2. Show that the language $\Sigma_i SAT$ definedin the book (5.2) is complete for Σ_i^p under polynomial-time reductions.

Problem 3.3. Define the class DP as the set of languages L such that there are two languages $L_1 \in NP$, $L_2 \in coNP$ such that $L = L_1 \cap L_2$. Note that this is *not* $NP \cap coNP$! Consider the problem

$$SAT\text{-}UNSAT = \{\langle \phi_1, \phi_2 \rangle \mid \phi_1 \text{is satisfiable}, \phi_2 \text{ is unsatisfiable}\}$$

Show that it is DP-complete under poly-time reductions. Show that EXACT-INDSET is DP-complete under poly-time reductions.

Problem 3.4. By writing out the truth table, you can compute any function by a circuit of size at most $O(n2^n)$. Here, we strengthen the result. First, show every function can be computed by a circuit of size $O(2^n)$ using Shannon's decomposition:

$$f(x_1, \ldots, x_n) = x_1 \wedge f(1, x_2, \ldots, x_n) \vee \neg x_1 \wedge f(0, x_2, \ldots, x_n)$$

[Shannon] Every function $f : \{0,1\}^n \to 0, 1$ can be computed by a circuit of size $O(2^n/n)$. [Hint: Apply the Shannon reduction k times (for a parameter k to be determined later) to get a representation

$$f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_{n-k}), h_2(x_1, \ldots, x_{n-k}), \ldots, h_{2^k}(x_1, \ldots, x_{n-k}), x_{n-k+1}, \ldots, x_n)$$

where $g(y_1, \ldots, y_{2^k}, x_{n-k+1}, \ldots, x_n)$ is a $(2^k + k)$-ary function that is computed by a circuit of size $O(2^k)$ and h_1, …, h_{2^k} are all $(n-k)$-ary Boolean functions. Suppose that there is a circuit H of size s and with 2^k outputs that computes *all* h_1, …, h_{2^k} simultaneously, then we can compute f by a circuit of size $s + O(2^k)$.

(1) Show that for each l, there is a circuit of size $O(2^{2^l})$ with 2^{2^l} outputs which computes all l-ary Boolean functions simultaneously. (Use induction to assume such a circuit exists for $l-1$ and use Shannon's decomposition.)

(2) Pick k such that $2^k > 2^{2^{n-k}}$. Show that this choice of k allows you to compute f with size $O(2^n/n)$.

Problem 3.5. We will prove that if $P = NP$ then there is a language in EXP that requires circuits of size $2^n/n$.

First, show that $P = NP$ implies $EXP = EXP^{PH}$.

Second, use the ideas in Kannan's theorem to find a function of high complexity using $EXP^{\Sigma_2^p}$: the lexicographically first truth table of the function such that the function requires a circuit of size $2^n/n$.

Problem 3.6. Iterated addition takes as input k n-bit numbers and computes their sum. Show that iterated addition is in NC^1. Show that multiplication of two n-bit numbers is in NC^1.

Problem 3.7. Read the alternate proof of PARITY not being in AC^0 using the switching lemma (Theorem 14.1 and its proof in the book.) (Nothing to submit for this problem!)

Problem 3.8. [Hard.] Describe a real number ρ such that given a random coin that comes up with "Heads" with probability ρ, a Turing machine can decide an undecidable language in polynomial time. [How will you recover the bits of ρ?]

Have a Good Holidays and a Happy New Year!