CS 351: Solutions to Problem Set 1

(1a) Show that if P = NP, then EXP = NEXP.

Let $L \in \mathrm{NTIME}[2^{n^c}]$. Then the language $L' = \{x0^{2^{|x|^c}} \mid x \in L\}$ belongs to NTIME$[n]$, so by the hypothesis P = NP, belongs to DTIME$[n^a]$ for some a. Given x, to decide if $x \in L$, it is enough to decide if $x0^{2^{|x|^c}} \in L'$, which can be accomplished in time $O(2^{a|x|^c})$, so $L \in$ EXP.

(1b) Show that $\mathrm{E} = \bigcup_{c>0} \mathrm{DTIME}[2^{cn}]$ is not closed under polynomial-time reductions, that is, there are problems A and B such that A is polynomial-time reducible to B, $B \in$ E, but $A \notin$ E.

Pick $A \in \mathrm{DTIME}[2^{n^2}] \setminus \mathrm{DTIME}[2^{n \log n}]$; by the time hierarchy theorem, such an A exists, and we have $A \notin$ E. Let $B = \{x0^{|x|^2} \mid x \in A\}$. Clearly, $A \leq_{\log} B$ via the reduction that maps x to $x0^{|x|^2}$. Also, since $A \in \mathrm{DTIME}[2^{n^2}]$, we have $B \in \mathrm{DTIME}[2^n]$ (the algorithm: given y, if y is not of the form $x0^{|x|^2}$, reject, else accept y iff $x \in A$, and the latter task can be done in time $2^{|x|^2} = O(2^{|y|})$).

(1c) Use (1b) with suitable observations to show that NP $\neq$ E.

The class NP is closed under reductions: Suppose $A \leq_{\log} B$ via a reduction f computable in time n^a and that $B \in \mathrm{NTIME}[n^b]$, that is, B has a proof system R_B where the proof length and the verifier's running time are bounded by n^b. A proof system R_A for A can now be defined in the following way: $(x, y) \in R_A$ iff $(f(x), y) \in R_B$. It is easy to see that the proof length and verification time for R_A are bounded by n^{ab}, whence we have that $A \in$ NP.

Since NP is closed under reductions and E is not, we have NP $\neq$ E.

(2c) Problem 9.5.4(a) in the book: Show that the special case of SAT in which each variable can only appear twice is in P.

Given a formula φ, we will apply a sequence of simplifications. If any variable x of φ appears only once in clause C, set x to TRUE or FALSE so as to satisfy C, and set each of the other variables y in C to satisfy the clause other than C, if any, that y appears in. Delete all satisfied clauses. Similar if the occurrences of a variable are either both positive or both negated. Now we have a formula (which we will also call φ) where each variable appears twice, once negated and once positively (and not together in the same clause). At this point, it is convenient to translate this problem into one about graphs: define a graph G where each clause of φ is a vertex, and two clauses C_1 and C_2 share an edge if some variable x appears in C_1 and in C_2. In terms of G, φ is satisfiable iff the edges of G can be oriented so that every vertex has at least one incoming edge. Now repeatedly apply the following two steps: (1) If G has a cycle Y, orient the edges of Y either "clockwise" or "anti-clockwise" so that all the vertices on Y now have incoming edges; (2) While there is any vertex v that has an incoming edge, for every un-oriented edge (v, w), orient the edge towards w. When these two steps can be no longer carried out, we have an acyclic undirected graph, that is, a forest. It is clear that G can be successfully oriented iff the forest is empty.

(3a) A *combinatorial rectangle* (often, simply a *rectangle*) in $X \times Y$ is a subset $R \subseteq X \times Y$ such that $R = A \times B$ for some $A \subseteq X$ and $B \subseteq Y$. Prove that $R \subseteq X \times Y$ is a rectangle if and only if for every $x_1, x_2 \in X$ and $y_1, y_2 \in Y$, we have: $(x_1, y_1) \in R$ and $(x_2, y_2) \in R \implies (x_1, y_2) \in R$ and $(x_2, y_1) \in R$.

Let $R = A \times B$. If $(x_1, y_1) \in R$ and $(x_2, y_2) \in R$, since $R \subseteq A \times B$, we have $x_1, x_2 \in A$ and $y_1, y_2 \in B$. Since $R \supseteq A \times B$, we have $(x_1, y_2) \in R$ and $(x_2, y_1) \in R$.

Conversely, assume that whenever $(x_1, y_1) \in R$ and $(x_2, y_2) \in R$, also $(x_1, y_2) \in R$ and $(x_2, y_1) \in R$. Define $A = \{x \mid (\exists y)(x, y) \in R\}$ and $B = \{y \mid (\exists x)(x, y) \in R\}$. Clearly, $R \subseteq A \times B$. To show that $R \supseteq A \times B$, let $x \in A$ and $y \in B$. Since $x \in A$, there is some y' such that $(x, y') \in R$. Since $y \in B$, there is some x' such that $(x', y) \in R$. Since $(x, y') \in R$ and $(x', y) \in R$, we have $(x, y) \in R$.

(3b) Let $\mathcal{P}$ be a protocol and v be a node of the protocol tree. Let R_v denote the set of inputs (x, y) that reach node v. Prove that for every v, R_v is a combinatorial rectangle.

By induction. The base case: if $\mathcal{P}$ is a protocol over domain $X \times Y$, and if v is the root of the protocol tree, we have $R_v = X \times Y$, which is a combinatorial rectangle. Induction step: assume that R_v is the rectangle $X_v \times Y_v$, and consider the children $v0$ and $v1$ of v. Wlog. let v be a node labeled by a function $a_v : X \longrightarrow \{0,1\}$. Then $R_{v0} = \{(x, y) \in X_v \times Y_v \mid a_v(x) = 0\} = \{x \in X_v \mid a_v(x) = 0\} \times Y_v$, and $R_{v1} = \{(x, y) \in X_v \times Y_v \mid a_v(x) = 1\} = \{x \in X_v \mid a_v(x) = 1\} \times Y_v$, both of which are rectangles.

(3c) Show that any protocol that computes the equality function $\text{EQ} : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$, defined by $\text{EQ}(x, y) = 1$ if and only if $x = y$, must have at least 2^n leaves; since EQ has a trivial protocol of cost $2n$, it follows that the communication complexity of EQ is $\Theta(n)$.

Consider the set of inputs $\{(x, x) \mid x \in \{0,1\}^n\}$. We claim that no two inputs from this set can have the same transcript under any protocol $\mathcal{P}$ that computes EQ, that is, no two inputs from this set can reach the same leaf of the protocol tree. Suppose $\mathcal{P}(x, x) = \mathcal{P}(y, y) = \tau$ for $x \neq y$. The leaf τ must be labeled '1' since $\text{EQ}(x, x) = \text{EQ}(y, y) = 1$. However, by the rectangle property of communication protocols, we have $\mathcal{P}(x, y) = \mathcal{P}(y, x) = \tau$, which contradicts the assumption that $\mathcal{P}$ correctly computes EQ, since $\text{EQ}(x, y) = \text{EQ}(y, x) = 0$.

(3d) Consider the set $\{x0^n y \mid x, y \in \{0,1\}^*, |x| = |y| = n, y = x^R\}$, a subset of PAL, where x^R denotes the bitwise reversal of x. Show that if there is a multitape TM that solves PAL in time $T(n)$ and using space $S(n)$, then there is a communication protocol for the EQ problem of cost at most $O(TS/n)$.

We will assume that such a TM M exists, and present a protocol to compute EQ. Alice is given $x \in \{0,1\}^n$, Bob is given $y \in \{0,1\}^n$. Alice starts simulating M on the input $x0^n y^R$. Note that she can start this simulation even though she doesn't have y available; in fact, she can carry out the simulation until the input tape head of M scans past all of x and 0^n and enters the "y" part of $x0^n y^R$. When this happens, Alice will write sufficient information on the blackboard so that Bob can continue the simulation. Specifically, she will write the state of M, all the work tape contents, and the positions of all tape heads. Note that this can be done by writing $O(S)$ bits. Bob then continues the simulation, and he can conduct the simulation until the input tape head of M enters the x part of the input $x0^n y^R$, at which time Bob writes down the configuration of M on the blackboard. Alice and Bob thus alternate in simulating M on $x0^n y^R$, until M halts and either accepts/rejects, which is also recorded on the blackboard. Notice that since M accepts precisely the set of palindromes, it will accept $x0^n y^R$ iff $x = y$, so Alice and Bob thus solve the equality problem. Finally, note that M runs in time $T(3n)$, and must spend at least n steps between any access to x and any access to y; thus the number of alternations of Alice and Bob in the protocol is at most $T(3n)/n$, and each time $O(S(3n))$ bits are communicated. By the communication lower bound for equality from (3c), we have $T(3n)S(3n)/n \geq cn$ for some absolute constant c, so $T(3n)S(3n) \geq cn^2$. Letting $N = 3n$, we have shown that on inputs of length N, $TS = \Omega(N^2)$.