Introduction to Computational Complexity
ES1 Solutions

1. First suppose f is in NP and let T be a nondeterministic Turing machine computing f in polynomial time. We can construct a deterministic Turing machine T' such that it takes input x and y and outputs what T would've outputted with x as an input, with choices of transition functions encoded in y (we don't need two input tapes for this since we can, for example, agree that even positions are supposed to be x and odd positions are y). Let g be the function computed by T'. Then it is not hard to see that $g \in P$ and we can pick y so that $g(x, y) = 1$ iff $f(x) = 1$ subject to the conditions in the size of y.

   On the other direction, suppose we are given g and p. Let T' be the Turing machine computing g in polynomial time. We can reverse the above process by constructing a nondeterministic Turing machine that, given x, tries to write down the corresponding y randomly and then computing $g(x, y)$. As $|y|= p(|x|)$ and $g \in$ P we see that this new Turing machine computes f in polynomial time.

2. Just because we can solve the decision problem in polynomial time, it doesn't mean we can solve the corresponding search problem in polynomial time; though this would follow from P=NP as was shown in lectures.

3. We need to check that the problem "Is n prime?" is in NP. We can assume $n > 2$ because we can check the case $n = 2$ separately. Let $g(n, a, p_1, \ldots, p_k)$ be the Boolean function defined to be 1 if and only if

   (1) $a^{n-1} \equiv 1 \pmod{n}$; and

   (2) $p_1, \ldots, p_k$ are the prime factors of $n - 1$; and

   (3) $a^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n}$ for all i.

   First we show that n is prime iff there is $a, p_1, \ldots, p_k$ such that $g(n, a, p_1, \ldots, p_k) = 1$. If n is prime then take a to a generator of the cyclic group $(\mathbb{Z}/n\mathbb{Z})^*$ and the p_i's to be the prime factors of $n-1$. Then (1) is satisfied by Fermat's little theorem, (2) is obviously satisfied, and (3) is satisfied since the order of a is $n - 1$.

   Conversely, suppose we have found $a, p_1, \ldots, p_k$ such that $g(n, a, p_1, \ldots, p_k) = 1$. As $n > 2$, we see that $aa^{n-2} \equiv 1 \pmod{n}$ so a has a multiplicative inverse and thus $a \in (\mathbb{Z}/n\mathbb{Z})^*$, i.e., a is coprime to n. In particular, the order of a divides the order of the group, which is $n-1$. So, if $|a|< n-1$, we see that $|a|$ divides $\frac{n-1}{p_i}$ for some i, contradicting (3); so by the hint we see that n is prime. Missing

4.

5. Suppose f