Lecture 10

September 19, 2005

1 Complexity Theory

We have seen that problems have varying hardness, but some problems have a "subproblem" that is easily checkable. For example:

- $SAT(\varphi)$: Is a given formula φ satisfiable?
- 3-colorability: Is a given graph 3-colorable?

A common characteristic shared by these problems is that it is "hard" to find a solution for them, but we can easily check whether a given solution is correct. In the case of $SAT(\varphi)$, if we are given a particular truth assignment τ, we have already developed a polynomial time algorithm $eval(\varphi, \tau)$ that deterministically decides if $\tau \models \varphi$. Thus, given a (possible) solution τ we can easily verify that φ is satisfiable (finding the appropriate τ is a different problem). Similarly for the 3-colorability problem, if we are given a particular coloring of the nodes, we can easily check every node to see whether its neighbors are all of a different color; if they are, the coloring we were given "testifies" that the graph has the desired property that makes it belong to the class of graphs with no monochromatic edges. In the literature, the example that helps determine if an instance of the problem has a solution is called a *witness* since it *witnesses* that the instance has the desired property. In the case of $SAT(\varphi)$, the witness is the truth assignment τ.

The above problems also have a common formulation: they both aim at answering a question of the form: *Given an instance of an object, does it satisfy certain property?*. There are other types of problems that cannot be stated in this way, for example:

- *Chess*: In a chess game, does white always win?

For this kind of problem, we cannot get a solution easily (in fact, it is very difficult to even state the problem formally, which would require a discussion on game theory and assumptions on the opponent's strategy). Next we formally define a *decision problem*.

Definition 1 (Decision Problem). *Given a finite alphabet* Σ*, a* Decision Problem *is some language* $L \subseteq \Sigma^*$*. It is* nontrivial *if* $L \neq \emptyset$ *and* $L \neq \Sigma^*$*.*

Thus we know SAT and 3-colorability are decision problems, while the *Chess* problem is not. We can think of the first two problems as decision problems where x is a string encoding an instance of the problem, and L is the language of all instance encodings that have some property P.

As part of the exhaustive algorithms that solve the above problems, we have a *subproblem*: given a candidate witness y, does y make x have property P? This subproblem can be formalized as a decision problem by itself as follows: "Does $(x, y) \in L_P$, where L_P is the language of all strings (x, y) where y makes x have property P ?" For our previous examples, this subproblem is decidable in polynomial time. Often, the subproblems need not be formalized, i.e. it will suffice to say "... and checking if a witness y makes x have property P is easy..."

To make matters more clear, going back to our 2 examples we have:

- L_{SAT} is the language of all satisfiable formulas $x \in \Sigma^*$, where Σ is the set of all valid formula symbols (propositions, connectives and parentheses). A formula $\varphi \in L_{SAT}$ iff φ has property P*: φ is satisfiable.* One way to see if $\varphi \in L_{SAT}$ is to use some truth assignment τ that witnesses that φ has property P, which is decidable in polynomial time by $eval(\varphi, \tau)$.

- L_{3C} is the language of all 3-colorable graphs x (here assume that x is some valid encoding of a graph using some alphabet Σ that makes x unambiguous). Thus, a particular graph $G \in L_{3C}$ iff G has property P*: there is a 3-coloring for G that makes all of its edges non-monochromatic.* Again, one way to check if $G \in L_{3C}$ is to provide some 3-coloring of the vertices of G. It is decidable in polynomial time if the witness is a valid 3-coloring of G.

1.1 The NP Class

In the previous examples we recognized that we have at our disposal a polynomial time algorithm to solve the subproblem, i.e. to check whether a particular witness y makes x have property P. The question that arises immediately is: *how do we come up with a candidate solution?.* The search space for these candidate solutions is exponential in the size of the problem for the above examples, so it becomes increasingly time consuming to try them all.

Note, however, that if we could "magically guess" a candidate solution, we could check it efficiently. These problems are said to belong to the **NP** class of problems, which stands for **Nondeterministic Polynomial time**. "Magically guessing" here means *nondeterministically selecting* a candidate; and once we have one, it can be checked in polynomial time. Alternatively, we can say that a problem in **NP** can be solved in polynomial time by a *nondeterministic algorithm* that first *guesses* a witness and then checks it. Now we are ready to introduce a formal definition for the **NP** class of problems.

Definition 2 (NP). *A decision problem $L \in \Sigma^*$ is in NP if there exist:*

- *a polynomial P, and*
- *a polynomial time algorithm $A(x, y)$,*

such that $x \in L$ iff $\exists\ y \in \Sigma^{\leq P(|x|)}$ where $A(x, y) = 1$.

Where $\Sigma^{\leq k}$ is the set of all strings of length less than or equal to k. In other words, a decision problem is in **NP** if when we are given a "short" witness y, a polynomial time algorithm $A(x, y)$ exists to check if the witness makes x have the desired property. Formally, $A(x, y)$ is a membership indicator of (x, y) to the subproblem language, so we have $A(x, y) = 1$ iff y is a witness for x.

Example 1 ($SAT(\varphi)$)**.** *For the case of $SAT(\varphi)$, we saw that $L = L_{SAT}$, x is φ, the witness y is τ, and the algorithm $A(x, y)$ is $eval(\varphi, \tau)$ which takes polynomial time.*

The restriction that $y \in \Sigma^{\leq P(|x|)}$ ensures that the witness is "short enough" so that the checking algorithm $A(x, y)$ is guaranteed to always take polynomial time. This is important because there may be problems where the witness cannot be guaranteed to have a length bounded by $P(|x|)$, and thus it could not be shown that $A(x, y)$ takes polynomial time.

In the following examples the particular L, A, x and y will not be explicitly pointed out to encourage the reader to formalize them.

1.2 Some Examples

We present some well known problems with a short analysis:

Example 2 (Diophantine equation). *Does $P(x_1, x_2) = 0$ have integer solutions?*

The solution is undecidable because we cannot bound the size of x_1 and x_2. Hilbert's 10th problem asked if a technique for solving a general Diophantine existed. The impossibility of obtaining a general solution was proved by Matyasevich in the early 1970's. However, verifying the correctness of a particular solution (x_1', x_2') takes only polynomial time. This problem is not in NP, because short witnesses may not exist.

Example 3 (Compositness Problem). *Given a number $n \in N$, is n composite?*

Given two factors n_1 and n_2, it is easy to verify if $n = n_1 n_2$. However, the time taken to find suitable n_1 and n_2 is exponential on the length of the binary representation of n. This problem is in NP. However, in this particular case we can be a little more precise. In 2002 it was shown that this problem is also in the class PTIME, which is a subclass of NP.

Example 4 (Eulerian Cycle on graph $G(V, E)$). *Is there a bijective mapping $P : E \to \{1, \ldots, |E|\}$ such that if $P(e_2) = (P(e_1) + 1) \pmod{|E|}$ then there exist vertices $u, v, w \in V$ such that $e_1 = (u, v)$ and $e_2 = (v, w)$?*

An Eulerian Cycle on a graph G is a cycle that visits each edge exactly once. An Eulerian Cycle exists iff the degree of each node in the graph is even. Thus, this problem is not only in NP, it is in fact in PTIME.

Example 5 (Hamiltonian Cycle on graph $G(V, E)$). *Is there a bijective mapping $P : V \to \{1, \ldots, |v|\}$ such that if $P(v) = (P(u) + 1) \bmod |V|$, then $(u, v) \in E$?*

A Hamiltonian cycle on a graph G is a cycle that visits each node exactly once and terminates at the initial node. This problem is in NP.

Example 6 (k-Coloring Problem). *Consider a graph representation of a map. $G = (V, E)$, whose nodes are the partitions in the map and neighboring partitions (nodes) are connected by edges. A k-*coloring *is a mapping $C : V \mapsto \{1 \ldots k\}$, obeying the constraint $C(u) = C(v)$ only if $(u, v) \notin E$. We say G is k-colorable if it has a k-coloring.* Graph k-colorability *is the problem if checking whether a given graph is k-colorable.*

Graph k-colorability is also in NP. The witness is the k-coloring C.

Example 7 (Perfect Matching on graph $G(V, E)$). *Is there a subset E' of E such that every node is touched by one edge of E'?*

This problem is in NP. It is in fact also in PTIME.

Note that some problems that look very similar to each other may belong to different complexity classes, e.g. one may be in P and other in NP. A classical example is 2-coloring and 3-coloring of a graph. Finding if a graph can be colored by 2 colors is easy but doing the same with 3 colors is hard.

Note that an upper and lower bound for NP problems can easily be provided:

- NP $\subseteq$ EXPTIME since the problem can be solved by trying all possibilities.
- PTIME $\subseteq$ NP since an NP problem has at least the complexity of $A(x, y)$ which is in PTIME.

The NP class lies somewhere between polynomial and exponential time.

2 Complexity Hierarchy

We have seen the complexity classes for deterministic algorithms *(Deterministic Hierarchy)*:

$$LOGSPACE \subseteq PTIME \subseteq PSPACE \subseteq EXPTIME \subseteq EXPSPACE$$

After introducing *nondeterminism*, which is the ability to *guess*, we get nondeterministic algorithms and nondeterministic complexity classes with the following relationships:

$NLOGSPACE \subseteq NPTIME \subseteq NPSPACE \subseteq NEXPTIME \subseteq NEXPSPACE$

Now by combining the above two hierarchies, we get the following full hierarchy of complexity classes with interleaved deterministic and non-deterministic classes:

$$LOGSPACE \subseteq NLOGSPACE \subseteq PTIME \subseteq NPTIME \subseteq \dots$$

$$\dots \subseteq PSPACE \subseteq NPSPACE \subseteq EXPTIME \subseteq NEXPTIME \subseteq \dots$$

$$\dots \subseteq EXPSPACE \subseteq NEXPSPACE$$

It is known that exponential gaps lead to strict containment:

$LOGSPACE \subset PSPACE \subset EXPSPACE.$
$NLOGSPACE \subset NPSPACE \subset NEXPSPACE.$
$PTIME \subset EXPTIME.$
$NPTIME \subset NEXPTIME.$

Theorem 1 (Savitch's theorem). *$PSPACE = NPSPACE$ and $EXPSPACE = NEXPSPACE$*

3 Reducibility

Finally, we turn our attention to a very important tool that will allow us to relate problems to other "similar" problems.

Definition 3 (Polynomial Reduction). *Let $L_1, L_2 \subseteq \Sigma^*$. We say that L_1 is* polynomially reducible *to L_2, denoted $L_1 \leq_p L_2$ if there exists a PTIME-computable function $f : \Sigma^* \to \Sigma^*$, such that $x \in L_1$ iff $f(x) \in L_2$.*

Example 8. *Let L_+ be a language such that $(a, b, c) \in L_+$ iff $a + b = c$. Similarly, let L_- be the language such that $(a, b, c) \in L_-$ only iff $a - b = c$. To reduce L_+ to L_- we have $f(a, b, c) = (b, c, a)$, where f is the function that reduces an instance of L_+ to L_-.*

When we say that $L_1 \leq_p L_2$, it intuitively means that L_2 is at least as hard as L_1, or more clearly, that L_1 is no harder than L_2. Hardness here means that if we solve the decision problem for L_2, we can use the function f to solve the decision problem for L_1.

Definition 4 (NP-hard). *A decision problem $L \subseteq \Sigma^*$ is* NP-hard *if for every $L' \in NP$ we have $L' \leq_p L$.*

Note that this definition does not restrict L to be in NP, that is, L could be some language *harder* than NP.

Definition 5 (NP-Complete). *A decision problem $L \subseteq \Sigma^*$ is* NP-complete *if $L \in NP$ and L is NP-hard.*

Suppose $L_1, L_2 \in NPC$, then from the definition we know that $L_1 \leq_p L_2$, and also that $L_2 \leq_p L_1$. Then we say $L_1 \equiv L_2$, or, L_1 and L_2 are *inter-reducible.* Notice that $\leq_p$ is reflexive and transitive, but not symmetric. It defines a pre-order. Also, $\leq_p$ is an invariant of PTIME, that is, if $L_2 \in$ PTIME and $L_1 \leq_p L_2$, then $L_1 \in$ PTIME.

Note. *All NP-complete problems are polynomially equivalent.*

It is obvious that $P \subseteq NP$, but it is still unknown whether $P \subsetneq NP$. There are a lot of problems in NP for which we cannot find polynomial algorithms to solve so far. We also have the following theorems:

Theorem 2. *If $L \in NPC$, and $L \in PTIME$, then $P = NP$.*

This theorem states that if we can find a polynomial solution for *any* NPC problem, then all NPC problems become PTIME problems since they are all reducible to each other.

Another useful result is:

Theorem 3. *If $P \neq NP$, then $(NP - P) - NPC \neq \emptyset$*

This is known as Ladner's Theorem. It states that there are problems in NP that are neither NP-complete nor in P, where $(NP - P)$ is the set of problems that are *strictly* in NP (but not in P), provided that $P \neq NP$, which is still unknown.

In the next lecture we will continue our investigation of the complexity class NPC, and will consider its dual – co-NPC.