Lecture 4. Major Complexity Classes

4.1 Standard complexity classes

We first define the following standard complexity classes.

Definition 4.1 Time classes:

$$\mathrm{P} \;=\; \bigcup_{p:\mathrm{poly}} \mathrm{TIME}(p(\ell)), \qquad \mathrm{E} \;=\; \bigcup_{c>0} \mathrm{TIME}(2^{c\ell}), \qquad \mathrm{EXP} \;=\; \bigcup_{p:\mathrm{poly}} \mathrm{TIME}(2^{p(\ell)}).$$

Space classes:

$$\mathrm{PSPACE} \;=\; \bigcup_{p:\mathrm{poly}} \mathrm{SPACE}(p(\ell)).$$

The following relations are immediate from the definition.

Fact $\mathrm{P} \subseteq \mathrm{E} \subseteq \mathrm{EXP}$.

The class P is the class of polynomial-time solvable problems. In computational complexity theory, we would use the polynomial-time solvability as a rough/weak condition for the tractability. Thus, P can be considered as a class of tractable problems. We have the following simpler way to express this class.

Theorem 4.1

$$\mathrm{P} \;=\; \bigcup_{k\geq 1} \mathrm{TIME}(\ell^k) \;=\; \mathrm{TIME}(\ell^{O(1)}).$$

The following relation can be shown by simple simulation algorithms.

Theorem 4.2 $\mathrm{PSPACE} \;\subseteq\; \mathrm{EXP}$.

On the other hand, by using the Time Hierarchy Theorem, we can show the following separations.

Theorem 4.3 $\mathrm{P} \underset{\neq}{\subsetneq} \mathrm{E} \underset{\neq}{\subsetneq} \mathrm{EXP}$.

4.2 The class NP

The complexity classes defined so far are based on the computational resource needed to solve a given problem. On the other hand, the class NP is defined as a class of problems that can be characterized as follows. Recall that a decision problem is specified by a set of 'yes' input instances, i.e., a set of binary strings that need to get 'yes' answer given as an input of the problem.

Definition 4.2 A problem $L \subseteq \{0,1\}^*$ is in NP if there exist a polynomial q_L and a polynomial-time computable predicate R_L that satisfy the following for any $\ell \geq 1$ and any $x \in \{0,1\}^\ell$:

$$x \in L \;\Leftrightarrow\; \exists w\;[\;|w| \leq q_L(\ell) \;\wedge\; R_L(x,w)\;].$$

For each $x \in L$, a string w satisfying the right hand condition of the above is called a *witness* (for $x \in L$, or x being a positive instance for the problem L). The function q_L and R_L are respectively called a *witness bound* and a *verifier*.

Note that the condition of the above can be restated as follows:

$$\begin{array}{lll} x \in L & \Rightarrow & \exists w : |w| \le q_L(\ell)\ [\ R_L(x,w)\ ], \\ x \notin L & \Rightarrow & \forall w : |w| \le q_L(\ell)\ [\ \neg R_L(x,w)\ ]. \end{array} \tag{1}$$

Here are some examples of NP problems. We explain them in two categories.

Example 4.1

$$\begin{array}{lll} \text{HAM} & = & \{\ G\ :\ G \text{ is a Hamiltonian graph }\}. \\ \text{COR} & = & \{\ \langle G,k\rangle\ :\ G \text{ is } k\text{-colorable }\}. \\ \text{VC} & = & \{\ \langle G,k\rangle\ :\ G \text{ has a vertex cover of size } k\ \}. \\ \text{SAT} & = & \{\ F\ :\ F \text{ is a satisfiable (extended) Boolean formula }\}. \\ \text{3SAT} & = & \{\ F\ :\ F \text{ is a satisfiable 3CNF formula }\}. \\ \text{KNAP} & = & \{\ \langle\, \langle s_1,...,s_n\rangle, \langle c_1,...,c_n\rangle, B, K\,\rangle\ : \\ & & \quad \exists U \subseteq \{1,...,n\}\ [\ \sum_{u\in U} s_u \le B\ \wedge\ \sum_{u\in U} c_u \ge K\ ]\ \}. \\ \text{SSUM} & = & \{\ \langle\, \langle a_1,...,a_n\rangle, B\,\rangle\ :\ \exists U \subseteq \{1,...,n\}\ [\ \sum_{u\in U} a_u = B\ ]\ \}. \end{array}$$

Example 4.2

$$\begin{array}{lll} \text{EULER} & = & \{\ G\ :\ G \text{ is an Eulerian graph }\}. \\ \text{LP} & = & \{\ \langle A, \mathbf{b}, \mathbf{c}, z\rangle\ :\ \exists \mathbf{x} \ge \mathbf{0}\ [\ A\mathbf{x} \le \mathbf{b}\ \wedge\ \mathbf{cx} \ge z\ ]\ \}. \\ \text{PRIME} & = & \{\ n\ :\ n \text{ is a prime number }\}. \\ \text{COMPO} & = & \{\ n\ :\ n \text{ is a composite number }\}. \\ \text{GI} & = & \{\ \langle G_1, G_2\rangle\ :\ G_1 \text{ is isomorphic to } G_2\ \}. \end{array}$$

Note that the condition of the definition of NP (more clearly, the condition (1)) is not symmetric. Then by switching the 'yes' and 'no' conditions, we can define the symmetric notion as follows.

Definition 4.2 A problem $L \subseteq \{0,1\}^*$ is in coNP if there exist a polynomial q_L and a polynomial-time computable predicate R_L that satisfy the following for any $\ell \ge 1$ and any $x \in \{0,1\}^\ell$:

$$\begin{array}{lll} x \in L & \Rightarrow & \forall w : |w| \le q_L(\ell)\ [\ R_L(x,w)\ ], \\ x \notin L & \Rightarrow & \exists w : |w| \le q_L(\ell)\ [\ \neg R_L(x,w)\ ]. \end{array}$$

Note that it is easy to show that COMPO is in NP and also that PRIME is in coNP. We can also prove that both are in NP and coNP. In fact, it has been shown recently (well, 2002, already 14 years ago ;-) that PRIME is in P.

We can show the following relations between NP (and coNP) and standard complexity classes.

Theorem 4.4

$$\text{P}\ \subseteq\ \text{NP} \cap \text{coNP}\ \subseteq\ \text{EXP}.$$

Homework exercise from Lecture 4

Choose one of the basic problems and hand your answer in at the next class. (If you cannot attend the next class, you can submit your answer via email before the class.) You do not have to write a long answer. Usually one page is enough. I will decide OK or NG, and you can get one point by each OK answer. You can try one of the advanced problems. But since we have one week for the next class, even if you choose an advanced problem, due is the next class. As usual you can get two points by each OK answer to the advanced problem. (You cannot try both basic and advanced problems for each homework.)

* For writing an answer, you may use Japanese.

Basic problems

1. Solve the following two problems.
   (1) Following the definitions studied so far, prove the relation $\mathrm{P} = \mathrm{TIME}(\ell^{O(1)})$ stated in Theorem 4.1.
   (2) Prove HAM is in NP. (You need to specify concretely a verifier R_{HAM} and a witness bound polynomial $q_{\mathrm{HAM}}(\ell)$.)
2. For any constant k, consider any problem L in $\mathrm{SPACE}(\ell^k)$. Explain an algorithm for simulating L and that it runs in $\mathrm{TIME}(2^{c\ell^k})$ time for some c.
3. Prove that $\mathrm{P} \subsetneq \mathrm{E}$ stated in Theorem 4.3. (Hint: By the Hierarchy Theorem, we can show that, e.g., $\mathrm{TIME}(\ell^k) \subsetneq \mathrm{TIME}(2^\ell)$. But this is not enough to show the desired separation.)

An advanced problem

1. The witness size bound of all NP problems we showed in the class is linear (i.e., $O(\ell)$) with respect to the input length ℓ. Show an example that seems to need a nonlinear witness size bound. (Remark. Note that a natural witness for $G \in \mathrm{HAM}$ for any graph with n vertices is $O(n \log n)$, but this length is $O(\ell)$ in terms of the length of the binary description of G.)
2. All NP problems we showed in the class are all solvable in E. Show an example problem that seems to need, say, $O(2^{\ell^2})$-time to solve.
3. Prove that PRIME is in NP. (Please do not try to explain PRIME is in P; just showing in NP is enough.)