Lecture 5. Polynomial-time Reducibility

It seems difficult to who the absolute difficulty of certain NP problems; then researchers introduced a way to investigate their relative difficulties.

Definition 5.1 For any decision problems (or, sets of strings) A and B, we say that A is *many-one reducible* to B (abbrev. $A \leq_{\mathrm{m}} B$) if there exists a function h with the following properties. (h itself is called a *many-one reduction* (abbrev. $\leq_{\mathrm{m}}$-reduction).)
(a) h is a total function from $\{0,1\}^*$ to $\{0,1\}^*$,
(b) $\forall x \in \{0,1\}^*$ $[\ x \in A \ \Leftrightarrow\ h(x) \in B\ ]$, and
(c) h is computable.
If furthermore, h is polynomial-time computable, then we say that A is *polynomial-time many-one reducible* (abbrb. $A \leq_{\mathrm{m}}^{\mathrm{P}} B$).

Example 5.1 Define CLIWUE, IS, VC as follows. It is easy to see that CLIQUE is $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducible to IS. Conversely, IS is also $\leq_{\mathrm{m}}^{\mathrm{P}}$ to CLIQUE. Also IS and VC are $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducible to each other.

$$\begin{array}{lcl}
\text{CLIQUE} & = & \{\ \langle G, k\rangle\ :\ G \text{ has a clique of size } k\ \}.\\
\text{IS} & = & \{\ \langle G, k\rangle\ :\ G \text{ has an independent set of size } k\ \}.\\
\text{VC} & = & \{\ \langle G, k\rangle\ :\ G \text{ has a vertex cover of size } k\ \}.
\end{array}$$

Example 5.2 3SAT is $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducible to VC.

The following is the key property of $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducibility.

Theorem 5.1
(1) If $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ and B is in P then A is also in P.
(2) The same relation holds by replacing P with its super-classes such as NP, coNP, PSPACE, EXP, ..., etc.

From this theorem, we can discuss the relative hardness of two problems by using $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducibility. In fact, if $A \leq_{\mathrm{m}}^{\mathrm{P}} B$, then we have $B \in \mathrm{P} \Rightarrow A \in \mathrm{P}$, $B \in \mathrm{PSPACE} \Rightarrow A \in \mathrm{PSPACE}$, etc.; hence, we may consider that B's complexity bounds A's complexity, or A is no harder than B. That is,

$$A \ \leq_{\mathrm{m}}^{\mathrm{P}}\ B \quad \overset{\text{intuitively}}{\Longrightarrow} \quad \boxed{A\text{'s hardness} \leq B\text{'s hardness}}$$

Note that $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducibility satisfies the conditions for the preorder, i.e., the reflexibility and the following transitivity.

Theorem 5.2 If $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ and $B \leq_{\mathrm{m}}^{\mathrm{P}} C$, then $A \leq_{\mathrm{m}}^{\mathrm{P}} C$.

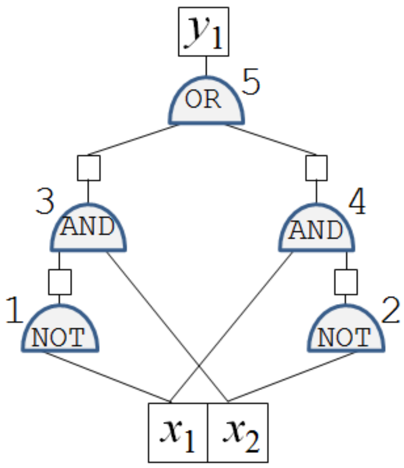
There is one important remark on the $\leq_{\mathrm{m}}^{\mathrm{P}}$-reduciblity. It can be used only for comparison based on the polynomial-time computability. We cannot use it for discussing the difference between, say, $O(\ell^2)$-computability and $O(\ell^4)$-computability. For exmple, we have the following fact.

Theorem 5.3 Let L_{trivial} be a trivial problem that determines whether a given input is 1 or not. Any problem in P is $\leq_{\mathrm{m}}$-reducible to such a trivial problem L_{trivial}.

The following examples are for preparing the next lecture.

Example 5.3 SAT is $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducible to 3SAT. Similarly the following CircuitSAT is $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducible to 3SAT.

CircuitSAT $=$ $\{\, C \,:\, C$ is a description of a Boolean circuit that has a satisfying assingment $\}$.



1	NOT	x_1		
2	NOT	x_2		
3	AND	1	x_2	
4	AND	x_1	2	
5	OR	3	4	y_1

Figure 5.1 An example of circuit description

Homework exercise from Lecture 5

Solve the following basic problems. (This time you need to solve the all three problems to get 1 point.) Due date is Oct. 16th (Mon.), the next class.

* For writing an answer, you may use Japanese.

Basic problems

1. Prove Theorem 5.1 (1).
2. Prove Theorem 5.1 (2) for NP.
3. Prove Theorem 5.2.