Lecture 6. NP-Completeness

Let us prove another key theorem in this course, that is, the NP-completeness of the SAT problem. We start by introducing the NP-completeness notion, and its basic properties.

Definition 6.1 A decision problem C is *NP-complete* if it satisfies the following properties.
(1) For any problem L in NP, we have $L \leq_{\mathrm{m}}^{\mathrm{P}} C$, and
(2) C is in NP.
Remark. A problem satisfying (1) is called *NP-hard*.

Theorem 6.1 Let C be any NP-complete problem. Then we have $C \in \mathrm{P} \Leftrightarrow \mathrm{P} = \mathrm{NP}$.

The theorem can be restated as follows:

$$C \notin \mathrm{NP} - \mathrm{P} \;\Leftrightarrow\; \mathrm{P} \neq \mathrm{NP}.$$

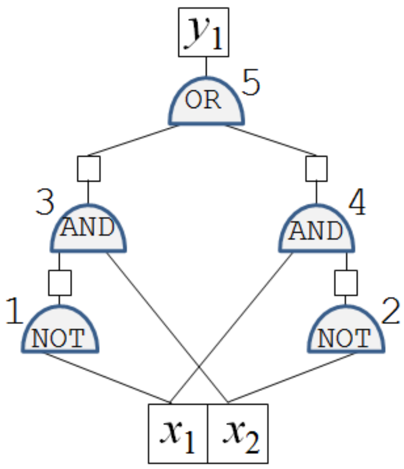
That is, C is the strongest candidate for a problem in $\mathrm{NP} - \mathrm{P}$.
By the transitivity of the $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducibility, we can show the NP-completeness in the following way.

Theorem 6.2 If $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ and A is NP-complete, then B is also NP-complete.

We know that 3SAT $\leq_{\mathrm{m}}^{\mathrm{P}}$ VC. Hence, if 3SAT is NP-complete, so is VC. Furthermore, since VC $\leq_{\mathrm{m}}^{\mathrm{P}}$ ISO and CLIQUE, they are also NP-complete. And indeed we will see that 3SAT is NP-complete.
We demonstrate some simple technique for the proof of our main theorem.

Example 6.1 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 assignment $\}$.



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 6.1 An example of circuit description

Now we prove our main theorem.

Theorem 6.3 CircuitSAT is NP-complete.

Thus, SAT and hence 3SAT are NP-complete.

Homework exercise from Lecture 6

Give an outline of the proof of Theorem 6.3. In particular, explain the following. Consider any problem L in NP. Then by definition, there exist a polynomial q_L and a predicate R_L that checks whether $x \in L$ by

$$x \in L \;\Leftrightarrow\; \exists w : |w| \le q_L(|x|)[\, R_L(x, w)\,],$$

where R_L is a polynomial-time computable predicate and $\mathtt{M}_L$ is a Turing machine computing R_L. Since CircuitSAT is NP-complete, there should be a $\le_{\rm m}^{\rm P}$-reduction from L to CircuitSAT. Consider any input x for the problem L. Explain what sort of circuit for the CircuitSAT problem is defined by the reduction on this x.

* For writing an answer, you may use Japanese.