COS 341, November 12, 1997
Handout Number 16

Reducibility Proof

Problem A is said to be *polynomial-time reducible* to Problem B if, for some fixed integer k, the following is true. Given an input I of size n for A, one can construct efficiently an input I' of size $\leq n^k$ for B such that the answer to I' is YES if and only if the answer to I is YES.

In this course when you are asked to show that A is polynomial-time reducible to B, we do not require a proof with complete details. However, it should contain at least the following elements.

First, the construction of I' from I should be unambiguous, and it has to be convincing that the size of I' is at most a polynomial function of the size of I'. (In principle, the construction needs to be doable in polynomial time, but we will not ask you to give a proof.)

Second, you need to give a convincing argument that the answer to I' is YES if and only if the answer to I is YES.

As an example, we show that the Eulerian cycle problem is polynomial-time reducible to the Hamiltonian cycle problem. Let $G = (V, E)$ be a graph where $|V| = n$ be the input to the Eulerian cycle problem. The size of G is the number of bits needed to encode V and E, and thus at most n^2.

We construct $G' = (V', E')$ as an input to the Hamiltonian cycle problem as follows. For each $e = \{i, j\} \in E$, construct three vertices $v_{e,i}, v_{e,j}, v_e$; let V' be the set of all such vertices. Thus, $|V'| = 3|E| \leq 3n^2$. There will be two kinds of edges in E': first, for each $e = \{i, j\} \in E$, create two edges $\{v_e, v_i\}$, $\{v_e, v_j\}$; second, for each $i \in V$, if there are s $e \in E$ incident to i in G, create all the $\binom{s}{2}$ edges among $v_{e,i}$ for these s e's. Note that the size of G' is at most $|V'|^2 \leq (3n^2)^2 = 9n^4$. Furthermore, the construction of G' can be done efficiently (this last assertion you don't need to justify rigorously for this course).

It remains to show that

Claim: G has an Eulerian cycle if and only if G' has a Hamiltonian cycle.

Let $m = |E|$. Suppose G has an Eulerian cycle $i_1, e_1, i_2, e_2, i_3, \cdots, i_m, e_m, i_1$ where $e_k \in E$ has i_k, i_{k+1} as its two endpoints. Then the following is clearly a Hamiltonian cycle in G' (just check that all vertices in V' appear, and that all consecutive vertices are connected by edges in E'):

$$v_{e_1,i_1}, v_{e_1}, v_{e_1,i_2}, v_{e_2,i_2}, v_{e_2}, v_{e_2,i_3}, \cdots, v_{e_m,i_m}, v_{e_m}, v_{e_m,i_1}, v_{e_1,i_1}.$$

This proves the claim in one direction.

Conversely, assume that G' has a Hamiltonian cycle C in which the $m = |E|$ vertices of the form v_e ($e \in E$) appear in the circular order $v_{e_1}, v_{e_2}, \cdots, v_{e_m}, v_{e_1}$. Note that, since each v_e has only two edges in E', these two edges must be used in the Hamiltonian cycle to enter and leave v_e. Since there are only $3m$ vertices in V', it follows that the cycle C must be of the form

$$v_{e_1,i_1}, v_{e_1}, v_{e_1,i'_1}, v_{e_2,i_2}, v_{e_2}, v_{e_2,i'_2}, \cdots, v_{e_m,i_m}, v_{e_m}, v_{e_m,i'_m}, v_{e_1,i_1},$$

where $e_k \in E$ has i_k, i'_k as its two endpoints in G. By definition of cycle, there must be an edge in E' connecting the two vertices $v_{e_t,i'_t}, v_{e_{t+1},i_{t+1}}$ for each $1 \leq t \leq m$, implying that $i'_t = i_{t+1}$. But this means that $i_1, e_1, i_2, e_2, i_3, \cdots, i_m, e_m, i_1$ is an Eulerian cycle in G. This proves the other direction.