Theory of Computation

Homework 4

Due: 2014/12/09

Problem 1 Show that VALIDITY is coNP-complete.

Proof: To show that VALIDITY is coNP-complete, it needs to show that VALIDITY $\in$ coNP and L can be reduced to VALIDITY for all $L \in$ coNP.

First, we can construct a TM which verifies the input x, and accepts if $x \in$ VALIDITY. Obviously, it takes polynomial time. So, VALIDITY $\in$ coNP.

Next, we show that L can be reduced to VALIDITY for all $L \in$ coNP. It is known that SAT is NP-complete. By Proposition 49 (See p. 444 in the slides.), $\overline{SAT}$ is coNP-complete. So, it suffices to show that $\overline{SAT}$ can be reduced to VALIDITY. Let N be an NTM which decides VALIDITY. Construct an NTM M which decides $\overline{SAT}$ as follows:

1: On input x, let $x' = \neg x$.

2: Run N(x')

3: If N accepts, halt and accept.

4: Otherwise, halt and reject.

M clearly runs in polynomial time. It completes the proof.

■

Problem 2 Recall that the Jacobi symbol is given by $(a|m) = \prod_i^k (a|p_i)$ for any odd integer $m = p_1 p_2 \ldots p_k$, $m > 1$, and $\gcd(a, m) = 1$. Show that $(-1|m) = (-1)^{(m-1)/2}$ for any odd integer m. (You may use the Legendre symbol $(a|p) = a^{\frac{p-1}{2}}$ for any odd prime p and $a \neq 0 \mod p$.)

Proof: Let n be an odd integer. Define

$$f(n) = \frac{n-1}{2} \mod 2. \tag{1}$$

Then we have

$$f(n) = \begin{cases} 0, & \text{if } n \equiv 1 \mod 4 \\ 1, & \text{if } n \equiv 3 \mod 4 \end{cases} \tag{2}$$

Moreover, for all odd integers a and b,

$$\begin{aligned} f(ab) - f(a) - f(b) &= \frac{ab - 1 - a + 1 - b + 1}{2} && (3) \\ &= \frac{(a-1)(b-1)}{2} && (4) \\ &\equiv 0 \mod 2. && (5) \end{aligned}$$

So, when a and b are odd primes, we have

$$\begin{aligned} (-1|ab) &= (-1|a)(-1|b) && (6) \\ &= (-1)^{f(a)}(-1)^{f(b)} && (7) \\ &= (-1)^{f(a)+f(b)} && (8) \\ &= (-1)^{f(ab)}. && (9) \end{aligned}$$

Assume that $m = p_1 p_2 p_3 \cdots p_k$ where p_is are odd primes but not necessarily distinct. Thus,

$$\begin{aligned} (-1|m) &= (-1|p_1)(-1|p_2)(-1|p_3)\cdots(-1|p_k) && (10) \\ &= (-1)^{f(p_1)}(-1)^{f(p_1)}(-1)^{f(p_3)}\cdots(-1)^{f(p_k)} && (11) \\ &= (-1)^{f(p_1)+f(p_2)+f(p_3)+\cdots+f(p_k)} && (12) \\ &= (-1)^{f(p_1 p_2 p_3 \cdots p_k)} && (13) \\ &= (-1)^{f(m)} && (14) \\ &= (-1)^{\frac{m-1}{2}}. && (15) \end{aligned}$$

■