Theory of Computation

Final-Term Examination on January 8, 2013
Fall Semester, 2012

Notes: You may use any results proved in the class unless stated otherwise. Recall:

- **RP**: If $L \in \mathbf{RP}$, then there exists a randomized polynomial-time TM M such that:
  - if $x \in L$, then at least half of the computation paths of M on x halt with "yes";
  - if $x \notin L$, then all computation paths halt with "no."
- **BPP**: If $L \in \mathbf{BPP}$, then there exists a randomized polynomial-time TM M such that:
  - If $x \in L$, then at least 3/4 of the computation paths of M on x lead to "yes";
  - If $x \notin L$, then at least 3/4 of the computation paths of M on x lead to "no."
- **IP**: If $L \in \mathbf{IP}$, then there exists an interactive proof system (P, V) such that the prover runs in exponential time and the verifier runs in probabilistic polynomial time and:
  - If $x \in L$, then the probability that x is accepted by the verifier is at least $1 - 2^{-|x|}$.
  - If $x \notin L$, then the probability that x is accepted by the verifier with any prover replacing the original prover is at most $2^{-|x|}$.

  Note that the number of rounds and the lengths of the messages are both polynomials in $|x|$. You can assume V sends out the first message.

Problem 1 (25 points) Prove (a) $\mathbf{RP} \subseteq \mathbf{BPP}$ and (b) $\mathbf{BPP} \subseteq \mathbf{PSPACE}$.

Ans:

(a) Let M be a randomized polynomial-time TM that recognizes $L \in \mathbf{RP}$ with one-sided error-probability ϵ. Assuming $\epsilon \leq 1/4$ does not affect $\mathbf{RP}$ (recall the slide on pp. 540). Thus the same TM M also recognizes L with two-sided error-probability ϵ.

(b) Let M be a randomized polynomial-time TM that recognizes $L \in \mathbf{BPP}$ with two-sided error-probability $\epsilon \leq 1/4$. Let $r(n)$ be the number of coin tosses of M. Then the following TM decides L:

Count of the number s of accepting paths.
If $s \geq (1-\epsilon)2^{r(n)}$, then accept; otherwise, reject.

By reusing space across executions of the loop in counting the number of accepting paths, this can be implemented in polynomial space.

■

Problem 2 (25 points) Please compute the Jacobi symbol (1003/1151). You need to write down the calculations instead of merely giving the answer. (Hint: Let p and q be two odd numbers (not necessarily primes). The law of quadratic reciprocity says $(p|q)(q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.)

Ans:

$$\begin{aligned}
(1003/1151) &= (-1)^{\frac{1003-1}{2}\frac{1151-1}{2}}(1151/1003) \\
&= -(1151/1003) \\
&= -(148/1003) = -(4/1003) \times (37/1003) \\
&= -(37/1003) = -(-1)^{\frac{37-1}{2}\frac{1003-1}{2}}(1003/37) \\
&= -(1003/37) \\
&= -(4/37) = -(2/37) \times (2/37) \\
&= -(-1)^{\frac{37^2-1}{8}} \times (-1)^{\frac{37^2-1}{8}} \\
&= -1.
\end{aligned}$$

■

Problem 3 (25 points) Define $\mathbf{IP}^*$ as $\mathbf{IP}$ except that the prover now runs in (deterministic) polynomial space instead of exponential time. Show that $\mathbf{IP}^* \subseteq \mathbf{PSPACE}$. (You cannot use the known fact $\mathbf{IP} = \mathbf{PSPACE}$.)

Ans: Let $L \in \mathbf{IP}^*$, (P, V) be an interactive proof system, V be a probabilistic polynomial-time verifier, P be a polynomial-space prover, c and k be some positive integers, n be the length of the input, $m_i \in \{0,1\}^*$ be ACCEPT/REJECT or the message sent in round i, and $r \in \{0,1\}^{n^k}$ be the random bit string in each round (for brevity, we had assumed r is of the same length in each round). Assume P and V interact for at most n^c rounds, and V accepts or rejects the input before or at round n^c. Construct deterministic TM M to simulate (P, V) as follows. Assume without loss of generality that V sends the first message. In the algorithm, t is the total number of choices for the random bits generated by V up to round i, and a is the number of choices for which V accepts up to round i. On any input x, M computes a and t recursively as follows by calling $\Gamma(x, 1)$:

Algorithm $(x, i, m_i, \ldots, m_{i-1})$

$(a, t) = (0, 0)$;
if $i = n^c$ **then**
 for all $r \in \{0,1\}^{n^k}$ **do**
  if $V(x, i, m_1, m_2, \ldots, m_{i-1}, r) =$ ACCEPT **then**
   $a = a + 1$;
  end if
 end for
 return $(a, 2^{n^k})$;
else
 for all $r \in \{0,1\}^{n^k}$ **do**
  $m_i = V(x, i, m_1, \ldots, m_{i-1}, r)$;
  if $m_i =$ ACCEPT **then**
   $(a, t) = (a + 1, t + 1)$;
  else if $m_i =$ REJECT **then**
   $(a, t) = (a, t + 1)$;
  else
   $m_{i+1} = P(x, i + 1, m_1, \ldots, m_i)$;
   $(a, t) = (a, t) + \Gamma(x, i + 2, m_1, \ldots, m_{i+1})$;
  end if
 end for
 return (a, t);
end if

Let $s = \frac{a}{t}$. If $s \geq 2/3$, then M accepts x; otherwise, M rejects x. This algorithm performs in polynomial space. So M decides L in polynomial space. ■

Problem 4 (25 points) Prove that there is no ϵ-approximation algorithm for 6-COLORING if ϵ <1/7 and assuming P $\neq$ NP. (Hint: Recall that an ϵ-approximation algorithm F guarantees that

$$OPT \leq c(F(G)) \leq \frac{OPT}{1-\epsilon}$$

where $c(F(G))$ is the number of colors the polynomial-time algorithm F uses to color G. What is the quality of the coloring scheme if you color the input graph using the alleged ϵ-approximation algorithm?)

Ans: We prove the problem by contradiction. We assume that there exists an ϵ-approximation algorithm F that colors the graph G in polynomial time. Given ϵ <1/7, F will color G with at most $x = \frac{OPT}{1-\epsilon} = 6$ in polynomial time if G is 6-colorable. That is, F can decide the answer "YES" or "NO" to NP-complete problem 6-coloring in polynomial time. However, we know that it is impossible to solve an NP-complete problem in polynomial time if P$\neq$NP. ■