Theory of Computation

Final Exam, 2015 Fall Semester,
1/12/2016

Note: Unless stated otherwise, you may use any results proved in class.

Problem 1 (25 points) Reduce 3SAT to INTEGER PROGRAMMING.

Ans: Let the variables in the 3SAT formula be $x_1, x_2, ..., x_n$. We will have corresponding variables $z_1, z_2, \ldots, z_n$ in our integer program. First, we restrict each variable z_i such that

$$0 \leq z_i \leq 1, \quad \text{for all } i.$$

Assigning $z_i = 1$ in the integer program represents setting $x_i =$ true in the 3SAT formula, and assigning $z_i = 0$ represents setting $x_i =$ false. For each clause such as $(x_1 \vee \overline{x_2} \vee x_3)$, we can rewrite it as the integer program:

$$z_1 + (1 - z_2) + z_3 > 0.$$

To satisfy this inequality, we must either set $z_1 = 1$ or $z_2 = 0$ or $z_3 = 1$, which means we either set $x_1 =$ true or $x_2 =$ false or $x_3 =$ true in the corresponding truth assignment. Assigning true/false to every x_i in all clauses, we then will have a set of input of INTEGER PROGRAMMING that is equivalent to the given set of input to 3SAT. ■

Problem 2 (25 points) For the Diffie-Hellman Secret-Key Agreement Protocol, Alice and Bob agree on a large prime p and a primivite root g of p (where p and g are public). Alice chooses a random a and Bob also chooses a random b.

1. (10 points) What are the values of α, β and the common key?
2. (15 points) For $p = 11$, $g = 2$, $a = 4$ and $b = 5$, what are the values of α, β and the common key?

Ans:

1. The values of α and β are

$$\alpha \equiv g^a \pmod{p},$$
$$\beta \equiv g^b \pmod{p},$$

   and the common key is

$$\alpha^b \equiv g^{ab} \equiv g^{ba} \equiv \beta^a \pmod{p}.$$

2. For $p = 11$, $g = 2$, $a = 4$ and $b = 5$, the values of α and β are

$$\alpha \equiv 2^4 \equiv 5 \pmod{11},$$
$$\beta \equiv 2^5 \equiv 10 \pmod{11},$$

   and the common key is

$$\alpha^b \equiv 2^{4\times 5} \equiv \beta^a \equiv 1 \pmod{11}.$$

$\blacksquare$

Problem 3 (25 points) Prove that NP $\subseteq$ ZPP, then NP $\subseteq$ BPP.

Ans: Assume NP $\subseteq$ ZPP. Pick any NP-complete language L. We only need to show that $L \in$ BPP. There exists an algorithm A that decides L in expected polynomial time, say $p(n)$. By Markov's inequality, the probability that the running time of A exceeds $3p(n)$ is at most $1/3$. Run A for $3p(n)$ steps to determine with probability at least $1 - 1/3 = 2/3$ whether the input belongs in L. We therefore obtain a polynomial-time algorithm for L which errs with probability at most $1/3$ on each input. Hence L is in BPP. $\blacksquare$

Problem 4 (25 points) Let $G = (V, E)$ be an undirected graph in which every node has a degree of at most k. Let I be a nonempty set. I is said to be independent if there is no edge between any two nodes in I. k-DEGREE INDEPENDENT SET asks if there is an independent set of size k. Consider the following algorithm for k-DEGREE INDEPENDENT SET:

$I := \emptyset$;
while $\exists v \in G$ **do**
    Add v to I;
    Delete v and all of its adjacent nodes from G;
end while;

6: **return** I;

Show that this algorithm for k-DEGREE INDEPENDENT SET is a $\frac{k}{k+1}$-approximation algorithm. Recall that an ϵ-approximation algorithm returns a solution that is at least $(1-\epsilon)$ times the optimum for maximization problems.

Ans: Since each stage of the algorithm adds a node to I and deletes at most $k+1$ nodes from G, I has at least $\frac{|V|}{k+1}$ nodes, which is at least $\frac{1}{k+1}$ times the size of the optimum independent set because the size of the optimum independent set is trivially at most $|V|$. Thus this algorithm returns solutions that are never smaller than $1 - \frac{1}{k+1} = \frac{k}{k+1}$ times the optimum. ■

Problem 5 (25 points) A cut in an undirected graph $G = (V, E)$ is a partition of the nodes into two nonempty sets S and $V - S$. MAX BISECTION asks if there is a cut of size at least K such that $|S| = |V - S|$. It is known that MAX BISECTION is NP-complete. BISECTION WIDTH asks if there is a bisection of size at most K such that $|S| = |V - S|$. Show that BISECTION WIDTH is NP-complete. You do not need to show it is in NP.

Ans: See pp. 392–393 in the slides. ■

Problem 6 (25 points) Is $x^4 \equiv 25 \bmod 1013$ solvable and why?

Ans:

Let's first notice that 1013 is a prime. Since 25 has square roots ± 5, we need to check if any of the Legendre symbols $\left(\frac{5}{1013}\right)$ or $\left(\frac{-5}{1013}\right)$ is 1. We have

$$\left(\frac{5}{1013}\right) = \left(\frac{1013}{5}\right) = \left(\frac{3}{5}\right) = -1$$

and

$$\left(\frac{-5}{1013}\right) = \left(\frac{-1}{1013}\right)\left(\frac{5}{1013}\right) = (-1)^{\frac{1013-1}{2}}\left(\frac{5}{1013}\right) = \left(\frac{5}{1013}\right) = -1$$

so 25 is not a quadratic residue modulo 1013 and cannot be a solution to $x^4 \equiv 25 \bmod 1013$. ■

Problem 7 (25 points) Let $n \in \mathbb{Z}^+$ with $n \geq 2$. Let $\phi(n)$ stand for Euler's totient function, which counts the number of positive integers smaller than n and are relative prime to n.

1. (5 points) Determine $\phi(2^n)$.

2. (10 points) Determine $\phi(\phi(2^n))$.

3. (10 points) Determine $\phi\left((2p)^n\right)$ where p is an odd prime.

Ans:

1. $\phi\left(2^n\right) = 2^n - 2^{n-1} = 2^{n-1}(2-1) = 2^{n-1}$.

2. $\phi\left(\phi(2^n)\right) = \phi\left(2^{n-1}\right) = 2^{n-1} - 2^{n-2} = 2^{n-2}(2-1) = 2^{n-2}$.

3. $\phi\left((2p)^n\right) = \phi\left(2^n p^n\right) = \phi\left(2^n\right)\phi\left(p^n\right) = 2^{n-1}(p^n - p^{n-1}) = 2^{n-1}p^{n-1}(p-1)$.

$\blacksquare$