CSC 364H **Problem Set 2** **Summer 99**

Due: day section: July 7, at 2:10 (in tutorial)
evening section: July 6, at 6:10 (in tutorial)

Note: Assignments are due at the *beginning* of tutorial, and late assignments are *not* accepted. The work that you submit *must* be your own. You may discuss problems with each other; however, you should take no notes during these discussions, and you should prepare written solutions alone.

1. Consider Freivalds' technique for checking whether $AB = C$, given three $n \times n$ matrices A, B, C (page 84 in the readings). Let $D = AB - C$, and let R be an $n \times 1$ column vector whose entries are chosen randomly and independently from the set $\{0, 1\}$. If $D = 0$, then $\Pr[DR = 0] = 1$, so the method never fails. On the other hand, if $D \neq 0$, then $\Pr[DR = 0] \leq 1/2$.

   (a) Suppose that the elements of R are chosen randomly (and independently) from the set $\{1, 2, 3\}$, instead of from $\{0, 1\}$. Suppose D has exactly one non-zero element. What is $\Pr[DR = 0]$ in that case? Give an example of a 2×2 matrix D such that $\Pr[DR = 0] = 1/3$.

   (b) Now suppose that the elements of R are chosen randomly from some fixed finite set S of elements. Show that if $D \neq 0$, then $\Pr[DR = 0] \leq 1/|S|$.

   (c) Show how to use Freivalds' technique to check whether $A^{-1} = B$, given matrices A, B.

2. Consider the method given in class for checking whether a given bipartite graph $G = (U, V, E)$ has a perfect matching, where U and V have n nodes each (page 89 in the readings). We suggested choosing values for the variables in the Edmonds matrix randomly from the set $\{1, 2, \ldots, n^2\}$, and in this case the probability of error is at most $1/n$. Suppose instead that each variable in the Edmonds matrix is replaced by a random k-bit integer (in binary notation). Give an upper bound for the probability of error in terms of k and n (do not use big-Oh notation). Evaluate your expression to two decimal places when $k = 16$ and $n = 100$.

3. Consider the Perfect Matching Decision Problem (PM): Given a bipartite graph G, determine whether G has a perfect matching. Show how to efficiently reduce the problem of actually finding a perfect matching in G (assuming it has one) to the decision problem PM. That is, assuming we are given a "black box" procedure PM(G) for solving the PM problem, give a polynomial time algorithm for finding the matching when it exists, where we do not count the time taken by calls to PM.

4. Recall that the Traveling Salesman Problem (TSP) is: Given n cities $\{1, 2, \ldots, n\}$, and a distance $D(i, j) \in \mathbb{N}$ between each pair (i, j) of cities, find a tour of minimum total

distance which starts and ends at city 1, and hits every other city exactly once. The tour can be represented by a sequence $\{1, \pi(2), \pi(3), \dots, \pi(n), 1\}$, where π is a permutation of the set $\{2, 3, \dots, n\}$.

Give a decision problem TSPD corresponding to the Traveling Salesman Problem TSP. Show that TSPD is in NP, and sketch an algorithm showing how to efficiently reduce TSP to TSPD.

5. Let the relation $R(x, y)$ hold iff x and y are finite strings over the alphabet $\{0, 1\}$, and x is an initial segment of y. (In particular, $R(x, y)$ holds if $x = y$.) Give a DTM which recognizes R. Assume that initially the strings x and y appear on the tape, separated by a blank square, and with blanks to the left of x and the right of y, and assume that initially the read/write head scans the left-most square of x (or b, if x is the empty string). Make sure that your DTM halts no matter what input strings x and y are given.

6. If $L \subseteq \Sigma^*$ then we use the notation $\overline{L}$ for the complement of L, that is $\overline{L} = \Sigma^* - L$.

   (a) Show that if $L \in \mathrm{P}$, then $\overline{L} \in \mathrm{P}$. Argue as follows: Suppose that M is a polytime DTM such that $L(M) = L$. Show how to modify M to form a polytime DTM M' such that $L(M') = \overline{L}$.

   (b) Suppose that a friend tries to convince you that if $L \in \mathrm{NP}$ then $\overline{L} \in \mathrm{NP}$ by the following argument: Let $R(x, y)$ be a polytime checking relation for L (i.e. $x \in L$ iff $\exists y\left[R(x, y) \text{ AND } |y| \leq c|x|^k\right]$ (for some fixed constants c and k). Then $\neg R(x, y)$ is a polytime checking relation for $\overline{L}$, where $\neg R(x, y)$ holds iff $R(x, y)$ does not hold.

   Show that your friend's argument is wrong, by giving a specific example of a language L with a polytime checking relation R, such that $\neg R$ is not a polytime checking relation for $\overline{L}$.

7. Let NSP (No Spanning Tree) be the following decision problem:

   Instance: Graph $G = (V, E)$, and edge cost function $c : E \longrightarrow \mathbb{N}$, and a number $B \in \mathbb{N}$.

   Question: Does every spanning tree T of G have cost $c(T) > B$?

   Either show that NSP $\in$ NP, or give a convincing argument that NSP $\notin$ NP.

8. Let ZERO SUM be the following decision problem:

   Instance: $d, w_1, \dots, w_d \in \mathbb{Z}$ (Note that we allow negative weights).

   Question: Is there a non-empty subset $S \subseteq \{1, \dots, d\}$ such that $\sum_{i \in S} w_i = 0$?

   Show that ZERO SUM is NP-complete, by doing the following two steps:

   (a) Show that ZERO SUM is in NP by giving a "guess and check" algorithm.

   (b) Show that PARTITION $\leq_p$ ZERO SUM.