CS 170 HW 15

Due on

1 Study Group

List the names and SIDs of the members in your study group.

2 Reduction Essentials

Assume A and B are search problems, and A reduces to B in polynomial time. In each part you will be given a fact about one of the problems. Determine what, if anything, this allows you to determine about the other problem. *Answer each part in one sentence.*

(a) A is in **P**

(b) B is in **P**

(c) A is **NP**-hard

(d) B is **NP**-hard

3 NP-complete problems

Prove that the following problems are NP-hard. In each case, specify which problem you are reducing from, which problem you are reducing to. Briefly, but precisely describe how you transform an instance of one problem to another.

(a) Directed Rudrata Cycle.
Input: A directed graph $G = (V, E)$.
Goal: Find a directed cycle that visits every vertex in V exactly once.

(b) Californian Cycle
Input: A directed graph $G = (V, E)$ with each vertex colored *blue* or *gold*, i.e., $V = V_{blue} \cup V_{gold}$. **Goal** Find a *Californian cycle* which is a directed cycle through all vertices in G that alternates between blue and gold vertices. (*Hint: Directed Rudrata Cycle*)

(c) 4-SAT
Input: n boolean variables $\{x_1,$
$ldots, x_n\}$ and clauses $\{C_1,$
$ldots, C_m\}$ with each having exactly

four distinct literals. For example, the following is an instance of $4 - SAT$.

$$(x_1 \vee x_2 \vee \overline{x_4} \vee \overline{x_5}) \wedge (x_3 \vee \overline{x_4} \vee \overline{x_1} \vee x_2) \wedge (x_1 \vee x_3 \vee x_4 \vee x_5)$$

. Note that all the 4 literals within a clause have to be distinct. **Goal:** Find an assignment to the variables $x_1, \ldots, x_n$ that satisfies all the clauses.

4 Hashing

Given a prime p and $a, b \in \{0, \ldots, p-1\}$, define the function $h_{a,b}(x) = ax + b \bmod p$ where $x \in \{0, \ldots, p-1\}$. Show that $H = \{h_{a,b}\}_{a,b \in \{0,\ldots,p-1\}}$ is a pairwise independent hash function family, i.e., show that for every $x \neq y$ and $c, d \in \{0, \ldots, p-1\}$ it holds that

$$\Pr_{h_{a,b} \leftarrow H} \Big[h_{a,b}(x) = c \wedge h_{a,b}(y) = d \Big] = \frac{1}{p^2} \ .$$

The notation $h_{a,b} \leftarrow H$ means that $h_{a,b}$ is chosen uniformly at random from H, meaning a and b are chosen independently uniformly at random from $\{0, \ldots, p-1\}$.

5 Streaming Algorithms

In this problem, we assume we are given an infinite stream of integers x_1,x_2, ..., and have to perform some computation after each new integer is given. Since we may see many integers, we want to limit the amount of memory we have to use in total. For all of the parts below, give a brief description of your algorithm and a brief justification of its correctness.

(a) Show that using only a single bit of memory, we can compute whether the sum of all integers seen so far is even or odd.

(b) Show that we can compute whether the sum of all integers seen so far is divisible by some fixed integer N using $O(\log N)$ bits of memory.

(c) Assume N is prime. Give an algorithm to check if N divides the product of all integers seen so far, using as few bits of memory as possible.

(d) Now let N be an arbitrary integer, and suppose we are given its prime factorization: $N = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$. Give an algorithm to check whether N divides the product of all integers seen so far, using as few bits of memory as possible. Write down the number of bits your algorithm uses in terms of $k_1, \ldots, k_r$.