CS 170 HW 14

Due **2020-12-07, at 10:00 pm**

1 Study Group

List the names and SIDs of the members in your study group. If you have no collaborators, you must explicitly write none.

In addition, we would like to share correct student solutions that are well-written with the class after each homework. Are you okay with your correct solutions being used for this purpose? Answer "Yes", "Yes but anonymously", or "No"

2 Nostalgia

What's been your favorite homework problem this semester? Tell us the HW number and problem name/number, and briefly explain (a sentence or two) why you liked it.

3 Super-Universal Hashing

Let $\mathcal{H}$ be a class of hash functions in which each $h \in \mathcal{H}$ maps the universe $\mathcal{U}$ of keys to $\{0, 1, \ldots, m-1\}$. Recall that $\mathcal{H}$ is *universal* if for any $x \neq y \in \mathcal{U}$, $\Pr_{h \in \mathcal{H}}[h(x) = h(y)] \leq 1/m$.

We say that $\mathcal{H}$ is super-universal if, for every fixed pair (x, y) of keys where $x \neq y$, and for any h chosen uniformly at random from $\mathcal{H}$, the pair $(h(x), h(y))$ is equally likely to be any of the m^2 pairs of elements from $\{0, 1, \ldots, m-1\}$. (The probability is taken only over the random choice of the hash function.)

(a) Show that, if $\mathcal{H}$ is super-universal, then it is universal.

(b) Suppose that you choose a hash function $h \in \mathcal{H}$ uniformly at random. Your friend, who knows $\mathcal{H}$ but does not know which hash function you picked, tells you a key x, and you tell her $h(x)$. Can your friend tell you $y \neq x$ such that $h(x) = h(y)$ with probability greater than $1/m$ (over your choice of h) if:

(i) $\mathcal{H}$ is universal?

(ii) $\mathcal{H}$ is super-universal?

In each case, either give a choice of $\mathcal{H}$ which allows your friend to find a collision, or prove that they cannot for any choice of $\mathcal{H}$.

4 Streaming Integers

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: $N = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$. 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 $k_1, \dots, k_r$.

5 Era of Ravens

(a) Design an algorithm that takes in a stream $z_1, \dots, z_M$ of M integers in $[n]$ and at any time t can output a uniformly random element in $z_1, \dots, z_t$. Your algorithm may use at most polynomial in $\log n$ and $\log M$ space. Prove the correctness and analyze the space complexity of your algorithm. Your algorithm may only take a single pass of the stream. *Hint:* $\frac{1}{t} = 1 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdots \frac{t-1}{t}$.

(b) For a stream $S = z_1, \dots, z_{2n}$ of $2n$ integers in $[n]$, we call $j \in [n]$ a *duplicate element* if it occurs more than once.

Design an algorithm that takes in S as input and with probability at least $1 - \frac{1}{n}$ outputs a duplicate element. Your algorithm may use at most polynomial in $\log n$ space. Prove the correctness and analyze the space complexity of your algorithm. Your algorithm may only take a single pass of the stream.

Hint: Use $\log n$ *copies of the algorithm from part a to keep track of a random subset of the elements seen so far. For proof of correctness, note that there are at most* n *indices* t *such that* $z_t \neq z_{t'}$ *for any* $t' > t$*, i.e. element* z_t *never occurs after index* t*.*

6 (Optional) Hadamard Gate

Please note that quantum computing is not in scope for the final.

Recall the Hadamard gate from the most recent homework, defined as follows:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

(a) Suppose we pass a 0 qubit through a Hadamard gate, and observe the output on the other end. With what probability will the observed output be 0? With what probability will the observed output be 1?

(b) What if we had passed in a 1 qubit instead?

(c) Briefly state how we might think to simulate this input/output behavior without the use of quantum gates.

(d) Verify that the Hadamard gate acts as its own inverse. What happens if we pass a 0 or 1 qubit through two Hadamard gates, and then observe the output?

(e) Why might the result to part (d) be surprising given the answer to part (c)?

7 (Optional) Quantum Gates

Please note that quantum computing is not in scope for the final.

(a) The Hadamard Gate acts on a single qubit and is represented by the following matrix:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Verify that this gate maps the basis states $|0\rangle$ and $|1\rangle$ to a superposition state that will yield 0 and 1 with equal probability, when measured. In other words, explicitly represent the bases as vectors, apply the gate as a matrix multiplication, and explain why the resulting vector will yield 0 and 1 with probabilities 1/2 each, when measured.

(b) Give a matrix representing a NOT gate. As in the previous part, explicitly show that applying your gate to the basis state $|0\rangle$ will yield the state $|1\rangle$ (and vice-versa).

(c) Give a matrix representing a gate that swaps two qubits. Explicitly show that applying this matrix to the basis state $|01\rangle$ will yield the state $|10\rangle$. Verify that this matrix is its own inverse.

8 (Extra Credit) The Power of Entanglement

Alice and Bob are playing the following game: A third party sends Alice x, which is 0 with probability 1/2 and 1 with probability 1/2. The third party also sends Bob y with the same distribution. Alice and Bob each choose a bit a, b. They win the game if $a \oplus b = x \wedge y$ ($a \oplus b$ is 0 if $a = b$ and 1 otherwise).

Alice and Bob are not allowed to communicate after receiving x, y, but they may come up with a shared strategy beforehand.

(a) Give a strategy for Alice and Bob that wins the game with probability 3/4.

(b) It turns out that without using quantum information, Alice and Bob can't come up with a strategy that wins with probability better than 3/4.

However, they can do better using quantum information. Consider the following strategy:

- Alice and Bob prepare two qubits in the state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Alice takes the first qubit, and Bob takes the second qubit. After this point, Alice and Bob won't communicate.

- Alice receives x and rotates her qubit by an angle of $\pi/8$ if $x = 1$. That is, she maps the state $|0b\rangle$ to the superposition of states $(\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle)|b\rangle$, and the state $|1b\rangle$ to the superposition of states $(-\sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle)|b\rangle$.
- Bob receives y and rotates his qubit by an angle of $-\pi/8$ if $y = 1$. That is, he maps the state $|a0\rangle$ to the superposition of states $|a\rangle(\cos(-\pi/8)|0\rangle + \sin(-\pi/8)|1\rangle)$, and the state $|a1\rangle$ to the superposition of states $|a\rangle(-\sin(-\pi/8)|0\rangle + \cos(-\pi/8)|1\rangle)$.
- Alice measures her qubit and chooses the bit she measures.
- Bob measures his qubit and chooses the bit he measures.

In the case that $x = 0, y = 0$, what is the probability Alice and Bob win using this strategy?

(c) In the case where $x = 1, y = 0$, what is the probability Alice and Bob win? This is also the probability they win if $x = 0, y = 1$, but you don't need to show this. You can give your answer rounded to three decimal places.

(d) Show that in the case where $x = 1, y = 1$, after rotating the qubits but before measuring, the qubits are in the superposition:

$$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle).$$

This implies Alice and Bob win in this case with probability $1/2$.

(The following equalities will be useful: $\cos(x) = \cos(-x), \sin(x) = -\sin(-x)$, and $\cos^2(\pi/8) - \sin^2(\pi/8) = 2\sin(\pi/8)\cos(\pi/8) = 1/\sqrt{2}$).

(e) Combining the previous three parts, what are Alice and Bob's overall chances of winning?