1 Hash tables

Hash tables with universal hash families guarantee an expected runtime of $O(1)$ for the INSERT, SEARCH, and DELETE operations. What is the meaning of “expected”? It is an average over the choices of the adversary who picks the elements in the table. Is it an average over the choices of the adversary who picks the elements in the table? It is an average over the choices of the algorithm who picks the hash function from the hash family.

In order to conclude an expected runtime of $O(1)$ for hash table operations, we assumed the following two facts in one or some order:

- The adversary picks elements $x_1, \ldots, x_n$ for the hash table.
- The algorithm picks a hash function from the hash family.

In order to do these happen?

- Algorithm first, and then adversary.
- Adversary first, and then algorithm.

It does not matter.

2 Bit lengths

Suppose that there is a top box with $N$ toys in it. You have a label printer that can print arbitrary strings of bits, and is. If you produce labels for the $N$ toys in such a way that each toy gets a unique label, what can be said about the longest label’s length?

- $\Theta(1)$
- $\Theta(\log N)$
- $\Theta(N)$
- $\Theta(1)$

As a remark, for any labeling scheme, the same lower bound of $\Omega(\log(N))$ applies even to the average label length, not just the longest label length. If you produce labels in a way that minimizes the longest label’s length, what is this minimum?

- $\Theta(\log N)$
- $\Theta(N)$
- $\Theta(1)$

If our toy box consists of all functions from $\{0, \ldots, M-1\}$ to $\{0, \ldots, n-1\}$, what is the minimum longest label’s length?

- $\Theta(N)$
- $\Theta(N\log N)$
- $\Theta(M)$

3 Modular arithmetic

Suppose that $M > 1000$ (the universe size) is a prime number. If we pick $a \in \{1, \ldots, M-1\}$ and $b \in \{0, \ldots, M-1\}$, independently and uniformly at random, what is $P_{a,b}(a \cdot x \equiv b \pmod{M})$?

- $\frac{1}{M}$
- $\frac{1}{M^2}$
- $\frac{1}{M}$

In fact, for any pair of distinct elements $x, y$ in the universe, $a = x \cdot x \equiv b \pmod{M}$ and $v = a \cdot v \equiv b \pmod{M}$ are uniformly distributed amongst all distinct pairs. How many elements of $\{0, \ldots, M-1\}$ are equal to $0$ modulo $a$?

- $\{0\}$
- $\{1, \ldots, M\}$
- $\{0\}$

In fact, for any $v$, the number of elements of $\{0, \ldots, M-1\}$ equal to $0$ modulo $a$ is $\leq \lfloor M/a \rfloor$. Let $a = 2^k$ be a power of two. What is the probability that $a \cdot v \equiv b \pmod{M}$?

- $\frac{1}{M}$
- $\frac{1}{M}$
- $\frac{1}{2^k}$

You can verify that this answer above is always $\leq 1/2$. The same answer holds as an upper bound if we changed a from 0 to any other element in $\{0, \ldots, M-1\}$.

4 Hash family size

Suppose that we have a universe of size $M$, and our hash table size is $N$. If $M \geq N$, what is the minimum size of a universal hash family?

- $1$