15-451/651 Algorithm Design & Analysis, Spring 2025

Recitation #2

Objectives

- Understand and review integer sorting algorithms, counting sort and radix sort
- Understand universal hash functions and their properties
- Review k-wise independent hashing and practice proving that a family is k-wise independent

Recitation Problems

1. **(Why is it called counting sort?)**

   (a) Suppose we are given an array of elements $a[0], \ldots, a[n-1]$ with integer keys in $0, \ldots, u-1$ to sort, and we have an array of *counts* $c[x]$ for each key x, i.e., a counter of how many times each element occurs in the input. An element $a[i]$ with key x at position i is in the correct sorted order if and only if what condition is true?

   (b) Using this idea, implement an algorithm that outputs the given array in **stable** sorted order by their integer keys $O(n+u)$ time and $O(n+u)$ space.

2. **(k-wise Independent Hashing)** Recall from class that a hash family $\mathcal{H}$ is *k-wise independent* if for all k distinct keys $x_1, x_2, \ldots, x_k \in \mathcal{U}$ and every set of k values $v_1, v_2, \ldots, v_k \in \{0, 1, \ldots, m-1\}$, we have that

$$\Pr_{h \in \mathcal{H}}[h(x_1) = v_1 \wedge h(x_2) = v_2 \wedge \cdots \wedge h(x_k) = v_k] = \frac{1}{m^k}$$

Intuitively, this means that if you look at only up to k keys, the hash family appears to hash them truly randomly.

(a) Is this hash family from $U = \{a, b\}$ to $\{0, 1\}$ (i.e., $m = 2$) universal? uniform (i.e., "one-wise independent")? how about pairwise (2-wise) independent?

	a	b
h_1	0	0
h_2	1	0

(b) Can you fill in the blanks in this hash family with values in $\{0, 1\}$ to make it pairwise independent? 3-wise independent?

	a	b	c
h_1	0	0	
h_2			1
h_3	0		
h_4	1	1	0

3. **(Extended Matrix Method)** In lecture we covered the *random binary matrix method* of hashing integers by interpreting them as binary vectors from the universe $\mathcal{U} = \{0,1\}^w$, into a table of size $m = 2^b$ indexed by $\{0,1\}^b$ where each hash function in the family is defined by a random matrix $A \in \{0,1\}^{b\times w}$ and

$$h(x) = Ax \mod 2$$

   (a) Prove that the matrix method is not 1-wise independent (i.e., not uniform).

   (b) Now suppose we extend the matrix method to be defined as

   $$h(x) = Ax + c \mod 2$$

   where $c \in \{0,1\}^b$ is a random binary vector.

   Prove that this extension of the matrix method is pairwise independent.