

CS 473 ✧ Spring 2016

☞ Homework 4 ☞

Due Tuesday, March 1, 2016, at 8pm

Unless a problem specifically states otherwise, you may assume a function `RANDOM` that takes a positive integer k as input and returns an integer chosen uniformly and independently at random from $\{1, 2, \dots, k\}$ in $O(1)$ time. For example, to flip a fair coin, you could call `RANDOM(2)`.

1. Suppose we are given a two-dimensional array $M[1..n, 1..n]$ in which every row and every column is sorted in increasing order and no two elements are equal.
 - (a) Describe and analyze an algorithm to solve the following problem in $O(n)$ time: Given indices i, j, i', j' as input, compute the number of elements of M larger than $M[i, j]$ and smaller than $M[i', j']$.
 - (b) Describe and analyze an algorithm to solve the following problem in $O(n)$ time: Given indices i, j, i', j' as input, return an element of M chosen uniformly at random from the elements larger than $M[i, j]$ and smaller than $M[i', j']$. Assume the requested range is always non-empty.
 - (c) Describe and analyze a randomized algorithm to compute the median element of M in $O(n \log n)$ expected time.
2. **Tabulated hashing** uses tables of random numbers to compute hash values. Suppose $|\mathcal{U}| = 2^w \times 2^w$ and $m = 2^\ell$, so the items being hashed are pairs of w -bit strings (or $2w$ -bit strings broken in half) and hash values are ℓ -bit strings.

Let $A[0..2^w - 1]$ and $B[0..2^w - 1]$ be arrays of independent random ℓ -bit strings, and define the hash function $h_{A,B}: \mathcal{U} \rightarrow [m]$ by setting

$$h_{A,B}(x, y) := A[x] \oplus B[y]$$

where \oplus denotes bit-wise exclusive-or. Let \mathcal{H} denote the set of all possible functions $h_{A,B}$. Filling the arrays A and B with independent random bits is equivalent to choosing a hash function $h_{A,B} \in \mathcal{H}$ uniformly at random.

- (a) Prove that \mathcal{H} is 2-uniform.
- (b) Prove that \mathcal{H} is 3-uniform. [Hint: Solve part (a) first.]
- (c) Prove that \mathcal{H} is **not** 4-uniform.

Yes, “see part (b)” is worth full credit for part (a), but only if your solution to part (b) is correct.