Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Dr. Alexander Souza
Thomas Janson

WS 2011/12
Sheet 03

Algorithm Theory

Exercise 1 (Randomized Quicksort) [Points: 6]

1. What is the running time of Quicksort when all elements of array A have the same value?
2. Show that the running time of Quicksort is $\Theta\left(n^2\right)$ when the array A contains distinct elements and is sorted in decreasing order.
3. One way to improve the Randomized Quicksort procedure is to partition around a pivot that is chosen more carefully than by picking a random element from the subarray. One common approach is the median-of-3 method: choose the pivot as the median (middle element) of a set of 3 elements randomly selected from the subarray. For this problem, let us assume that the elements in the input array $A\,[1..n]$ are distinct and that $n \geq 3$. We denote the sorted output array by $A'\,[1..n]$. Using the median-of-3 method to choose the pivot element x, define $p_i = \Pr\left\{x = A'[i]\right\}$.
   (a) Give an exact formula for p_i as a function of n and i for $i = 2, 3, ..., n-1$. (Note that $p_1 = p_n = 0$)
   (b) By what amount have we increased the likelihood of choosing the pivot as $x = A'\left[\left\lfloor \frac{n+1}{2} \right\rfloor\right]$, the median of $A[1..n]$, compared with the ordinary implementation? Assume that $n \to \infty$, and give the limiting ratio of these probabilities.
   (c) Argue intuitively that in the $\Omega\left(n \log n\right)$ running time of quicksort, the median-of-3 method affects only the constant factor.

Exercise 2 (RSA) [Points: 4]

For an RSA encryption choose $p = 17$, $q = 19$ and let $e = 7$.

1. Compute the number d and give the output of the executed extended-Euclid algorithm. In addition, compute the secret and public keys.
2. By using the public key, cypher the decimal message $M = 14$.

Exercise 3 (Treaps) [Points: 4]

1. Insert the keys f, g, h, e, b, a, c into an initially empty treap. The priorities of these keys are given in the table below.

keys	a	b	c	e	f	g	h	i	j	k
priority	12	23	2	7	4	6	14	22	19	15

For each of the insert operations, illustrate the state of the treap before and after every rotation.

Exercise 4 (Treaps) [Points: 6]

1. The *left spine* of a binary search tree T is the path from the root to the node with the smallest key. In other words, the left spine is the longest path from the root that consists only of left edges. Symmetrically, the *right spine* of T is the path from the root to the node with the maximum key. The *length of a spine* is the number of nodes it contains (including the root).

   Consider a treap T immediately after inserting node x. Let C be the length of the right spine of the left subtree of x. Let D be the length of the left spine of the right subtree of x. Prove that the total number of rotations that were performed during the insertion of x is equal to $C + D$.

We will now calculate the expected values of C and D. Without loss of generality, we assume that the keys are $1, 2, ..., n$, since we are comparing them only to one another.
For nodes x and y in treap T , where $y \neq x$, let $k = x.key$ and $i = y.key$. We define random variables

$$X_{ik} = \begin{cases} 1 & y \text{ is in the right spine of the left subtree of } x, \\ 0 & \text{otherwise.} \end{cases}$$

2. Show that $X_{ik} = 1$ if and only if $y.priority > x.priority$, $y.key < x.key$, and, for every z such that $y.key < z.key < x.key$, we have $y.priority < z.priority$.

3. Show that

$$\Pr\{X_{ik} = 1\} = \frac{(k-i-1)!}{(k-i+1)!} = \frac{1}{(k-i+1)\,(k-i)}$$

4. Show that

$$\mathrm{E}[C] = \sum_{j=1}^{k-1} \frac{1}{j\,(j+1)} = 1 - \frac{1}{k}$$