Institut for Matematik og Datalogi
Syddansk Universitet

October 30, 2020
JFB

DM551/MM851 – Algorithms and Probability – 2020
Lecture 12

Lecture, October 27, in U55

We finished section 13.5 in KT. Then, we analyzed the expected number of comparisons done by Randomized Quicksort, using section 7.4.2 of *Introduction to Algorithms*, 3rd edition, by Cormen, Leiserson, Rivest, and Stein (CLRS). We also covered section 13.9 in KT (without proofs).

Lecture, October 29, in U20

We will cover section 11.3.3 in CLRS.

Lecture, November 2, online

We will begin on network flows from chapter 26 in CLRS. There are slides for this topic. We will also do a midway evaluation.

Problems to be discussed on November 13

1. Compare the Chernoff bounds to what you would get using Chebyshevs inequality on the same random variables (the ones that Chernoff bounds apply to). Just do the case where you want to find out the probability of being less than the expected value. Note that you need to find an upper bound on the variance.

2. Exercise 2 on page 782 of Kleinberg and Tardos. Then compute an upper bound on the probability of at least 1000 Democrats voting for candidate R.

3. Consider the class of universal hash functions from section 11.3.3. Given $p = 37$, $m = 8$, let $a = 5$ and $b = 9$. Try hashing $k = 8$ and $\ell = 12$. Now find a key k' which will collide with $k = 8$ with this hash function.

4. Suppose you are using hashing for digital signatures. The idea is that you are signing very long messages, so you hash them down to some fixed size and then sign that hash value with digital signature scheme. For such a system to be secure it should not be possible to find a message which hashes to the same value as another message which has already been signed. The problem is that the same digital signature would work

on the new message. Show that the class of universal hash functions from section 11.3.3 in CLRS would not be good for use with digital signatures.

5. The proof that the class of universal hash functions is universal does not seem to consider the case where the set U does not contain all values in $\mathbb{Z}_p$. What if it contains fewer?

6. Do exercise 11.3-5 in CLRS.