Institut for Matematik og Datalogi
Syddansk Universitet

October 29, 2018
JFB

DM551 – Algorithms and Probability – 2018
Lecture 13

Lecture, October 29

We covered sections 5.4.3 and 5.4.4 in CLRS.

Lecture, November 5

We will cover section 11.3.3 in CLRS.

Lecture, November 6

We will cover sections 8.1 and 8.2 in Rosen.

Problems to be discussed on November 13

1. Exercises not covered yet.

2. 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.

3. 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.

4. 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?

5. Do exercise 11.3-5 in CLRS.