Practicals for Introduction to Approximation and Randomized Algorithms

WS2324 - 7. practical

1

Let us have a function $F : \{0, \dots, n-1\} \to \{0, \dots, m-1\}$.
We are told that $F((x+y) \mod n) = (F(x) + F(y)) \mod m$ holds for any $x, y \in \{0, \dots, n-1\}$.
The only way for us to evaluate F is by using a lookup table, in which the values of F are stored. However, $1/5$ of all values in this table are wrong and we don't know which.
Describe a simple randomized alorithm, which, for any given value of z, returns $F(z)$ with probability at least $1/2$.

Suppose that you are then allowed to run this algorithm three times for a given z. You will thus get three (not necessarily different) values, which should be $F(z)$. **With what probability can you determine $F(z)$ now?**

2

Show that $\mathrm{var}(X) \leq 1/4$ holds for any discrete random variable X that only has values in the interval $[0, 1]$.

3

We have seen in the lecture that, for any $p \geq n$ (where p is a prime) the family of hash functions

$$\mathcal{H} = \{h_{a,b} \mid 1 \leq a \leq p-1, 1 \leq b \leq p\}$$

where

$$h_{a,b}(x) = ((ax + b) \mod p) \mod n$$

is 2-universal.

Now consider a family of hash functions

$$\mathcal{H}' = \{h_a \mid 1 \leq a \leq p-1\}$$

where

$$h_a(x) = (ax \mod p) \mod n.$$

Show that this family is not 2-universal.
Then show that it is almost 2-universal in the sense that, for any $x, y \in \{0, \dots, p-1\}$ and for a uniformly randomly selected $h \in \mathcal{H}'$ we get $\Pr(h(x) = h(y)) \leq 2/n$.