Übungsblatt 5

Andrés Fernández Lebrón, af231
Mehmet Kaan Isik, mi84
Paramie Willmann, pw221

Aufgabe 1

a) As m increases, the value of the function will yield the same result, namely: 0. Thus, increasing the probability of keys having the same value.

b) As long as $x \geq (m-1)/2$, the probability of collision is almost certain. Thus, making this function not suitable (good).

c) The value of the function will repeat itself periodically. This repetition renders the function unsuitable.

d) The main problem of this function is the consistency. We want our hash function to give the same result for a given x every time, which this function would fail to do.

e) 1. Similar to (c), this function has the probability of x/0.
2. The division method consists in just one modular division, so that it is not clear why does the hash function have another modular division.
3. The chosen prime number is not assigned to m. That goes against the recommendation for choosing m as a prime number.

f) The main purpose of hashing is to reduce our asymptotic complexity to O(1), or in practice something close to it. By using this function we are increasing our time complexity, and therefore undermining our original purpose for using hashing.

Aufgabe 2

a) In order to show that h1 is not a c-universal hash function, it must be shown that h1 does not belong to a family of c-universal hash functions. In turn, to demonstrate this it must shown that h1 does not comply with the conditions of c-universality, namely:

$$\forall x, y \in S : x \neq y \Rightarrow |\{h \in H : h(x) = h(y)\}| \leq (c.|H|)/m$$

To show this, it must be shown that the ratio (i.e. probability) of collision for two keys (say x and y) is greater then c/m. Thus it should be shown (1) a collision and (2) that that collision's probability is equal or greater that c/m.

Collision of $h(x)$ and $h(y)$:
Let be x and $y = x + m$.
$h(x) = a.x^2 \bmod m$
$h(y) = a.(x + m)^2 \bmod m$
$h(y) = (a.x^2 + 2.x.m.a + a.m^2) \bmod m$
$h(y) = (a.x^2) \bmod m + (2x * m * a) \bmod m + (a.m^2) \bmod m$
$h(y) = (a * x * *2) \bmod m + 0 + 0$

Therefore $h(x) = h(y)$

Collision's probability $\geq c/m$
The probability parameter for a c-universal family of hash functions is $c/m|H|$. This may be simplified as c/m, since $((c/m) * (1/|H|)) = c/m$. Let be $c = 3$ (because it could be greater than 1) and $m = 11$.
Thus if c/m, then 3/11.
Now, Pr $(h(x) == h(y)) = 1/1$
Since 1 / 1 is greater than 3/11, the probability requirement does not hold.
Therefore, H1 does not comply with the condition of c-universality.

b)