



Algorithms and Datastructures

Winter Term 2022

Grading Guidelines Exercise Sheet 5

Due: Wednesday, November 23rd, 2pm

Exercise 1: Bad Hash Functions

(10 Points)

Let m be the size of a hash table and $M \gg m$ the largest possible key of the elements we want to store in the table. The following “hash functions” are poorly chosen. Explain for each function why it is not a suitable hash function.

- (a) $h : x \mapsto \lfloor \frac{x}{m} \rfloor \bmod m$ (1,5 Points)
- (b) $h : x \mapsto (2x + 1) \bmod m$ (m even). (1,5 Points)
- (c) $h : x \mapsto (x \bmod m) + \lfloor \frac{m}{x+1} \rfloor$ (1,5 Points)
- (d) For each calculation of the hash value of x one chooses for $h(x)$ a uniform random number from $\{0, \dots, m-1\}$ (1,5 Points)
- (e) $h : x \mapsto \lfloor \frac{M}{x \cdot p \bmod M} \rfloor \bmod m$, where p is prime and $\frac{M}{2} < p < M$ (2 Points)
- (f) For a set of “good” hash functions h_1, \dots, h_ℓ with $\ell \in \Theta(\log m)$, we first compute $h_1(x)$, then $h_2(h_1(x))$ etc. until $h_\ell(h_{\ell-1}(\dots h_1(x)))$. That is, the function is $h : k \mapsto h_\ell(h_{\ell-1}(\dots h_1(x)))$ (2 Points)

Exercise 2: (No) Families of Universal Hash Functions (10 Points)

- (a) Let $\mathcal{S} = \{0, \dots, M-1\}$ and $\mathcal{H}_1 := \{h : x \mapsto a \cdot x^2 \bmod m \mid a \in \mathcal{S}\}$. Show that \mathcal{H}_1 is not c -universal for constant $c \geq 1$ (that is c is fixed and must not depend on m). (4 Points)
- (b) Let m be a prime and let $k = \lfloor \log_m M \rfloor$. We consider the keys $x \in \mathcal{S}$ in base m presentation, i.e., $x = \sum_{i=0}^k x_i m^i$. Consider the set of functions from the lecture (week 5, slide 15)

$$\mathcal{H}_2 := \left\{ h : x \mapsto \sum_{i=0}^k a_i x_i \bmod m \mid a_i \in \{0, \dots, m-1\} \right\}.$$

Show that \mathcal{H}_2 is 1-universal.

(6 Points)

Hint: Two keys $x \neq y$ have to differ at some digit $x_j \neq y_j$ in their base m presentation.

Remark: Since m is prim, for each element $a \in \{1, \dots, m-1\}$ there exists an inverse element $b \in \{1, \dots, m-1\}$ of a modulo m i.e., $a \cdot b \equiv 1 \pmod m$.