Exercise 1: Bad Hash Functions \( (10 \text{ Points}) \)

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) \( h : x \mapsto \left\lfloor \frac{x}{m} \right\rfloor \mod m \) \( (1,5 \text{ Points}) \)

(b) \( h : x \mapsto (2x + 1) \mod m \) (\( m \) even). \( (1,5 \text{ Points}) \)

(c) \( h : x \mapsto (x \mod m) + \left\lfloor \frac{M}{x+1} \right\rfloor \) \( (1,5 \text{ Points}) \)

(d) For each calculation of the hash value of \( x \) one chooses for \( h(x) \) a uniform random number from \( \{0, \ldots, m-1\} \) \( (1,5 \text{ Points}) \)

(e) \( h : x \mapsto \left\lfloor \frac{M}{x+p \mod M} \right\rfloor \mod m \), where \( p \) is prime and \( \frac{M}{2} < p < M \) \( (2 \text{ Points}) \)

(f) For a set of “good” hash functions \( h_1, \ldots, h_\ell \) with \( \ell \in \Theta(\log m) \), we first compute \( h_1(x) \), then \( h_2(h_1(x)) \) etc. until \( h_\ell(h_{\ell-1}(\ldots h_1(x))\ldots) \). That is, the function is \( h : k \mapsto h_\ell(h_{\ell-1}(\ldots h_1(x))\ldots) \) \( (2 \text{ Points}) \)

Exercise 2: (No) Families of Universal Hash Functions \( (10 \text{ Points}) \)

(a) Let \( S = \{0, \ldots, M-1\} \) and \( H_1 := \{ h : x \mapsto a \cdot x^2 \mod m \mid a \in S \} \). Show that \( H_1 \) is not \( c \)-universal for constant \( c \geq 1 \) (that is \( c \) must not depend on \( m \)). \( (4 \text{ Points}) \)

(b) Let \( m \) be a prime and let \( k = \lceil \log_m M \rceil \). We consider the keys \( x \in S \) 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)

\[ H_2 := \left\{ h : x \mapsto \sum_{i=0}^{k} a_i x_i \mod m \mid a_i \in \{0, \ldots, m-1\} \right\}. \]

Show that \( H_2 \) is 1-universal.\(^1\) \( (6 \text{ Points}) \)

\(^1\)This exercise and the according lecture slide was changed. Originally it stated \( H_2 := \{ h : x \mapsto \sum_{i=0}^{k-1} a_i x_i \mod m \mid a_i \in \{0, \ldots, m-1\} \} \) and \( k = \lfloor \log_m M \rfloor - 1 \). We are sorry for the inconvenience.