

## Aufgabe 1.

a)  $h: x \mapsto \lfloor \frac{x}{m} \rfloor \bmod m$ .  $n \in \{0, \dots, m-1\}$

Wenn wir diese Hash-Funktion verwenden, werden wir viele Kollisionen haben, da es gilt:

$$x < k \cdot m \rightarrow (k-1) \bmod m$$

Z.B.:

Sei  $S_1 = \{0, 1, \dots, m-1\}$ . Es gilt:

$$x \in S_1 \Rightarrow x < 1 \cdot m \text{ und } \lfloor \frac{x}{m} \rfloor = 0, \text{ da } \frac{S_1}{m} < 1.$$

Da  $|S_1| = m$  gilt, verursachen alle Zahlen aus  $S_1$  m Kollisionen, da jede auf die Zeile 0 zeigt.

b)  $h: x \mapsto (2x+1) \bmod m$ ,  $m$  ist gerade.

Wenn wir diese Hash-Funktion verwenden, werden wir nur Elemente an ungeraden Adressen der Hashtabelle legen. D.h. wir verwenden nur  $\approx \frac{m}{2}$  Platz, was zu einer großen Anzahl von Kollisionen und Platzverschwendungen führt.

c)  $h: x \mapsto (x \bmod m) + \left\lfloor \frac{m}{x+1} \right\rfloor$ .

Die Term  $x \bmod m$  bildet  $x$  bereits in den Bereich  $[0, m-1]$  ab. Das Hinzufügen von  $\left\lfloor \frac{m}{x+1} \right\rfloor$  kann eine ungleichmäßige Verschiebung einführen.

Sei z.B.  $m=15$ ,  $x=14$ . Es gilt:

$$h(14) = 14 \bmod 15 + \left\lfloor \frac{15}{14+1} \right\rfloor = 14+1 = 15$$

$\Rightarrow x \in \{0, \dots, 15\}$ , aber nach der Definition von der Hashfunktion muss  $x \in \{0, \dots, m-1\}$  gelten.

d) Derselbe Schlüssel  $x$  kann jedes Mal zu unterschiedlichen Hash-Werten führen, was es unmöglich macht, gespeicherte Elemente zuverlässig zu finden.

e)  $h: x \mapsto \left\lfloor \frac{m}{(x-p) \bmod m} \right\rfloor \bmod m$ ,  $p$  prim,  $\frac{m}{2} < p < m$ .

Unregelmäßige Verteilung, viele Werte sind gleich 1.

f)  $h: x \mapsto h_f(h_{f-1}(\dots(h_1(x))\dots))$ .

Das verwenden mehrerer verschachtelter Hashfunktionen erhöht die Zeitkomplexität und kann es schwierig machen, eine gleichmäßige Verteilung zu erreichen.

## Aufgabe 2

a)  $S = \{0, \dots, M-1\}$ .  $H_1 := \{ h: x \mapsto a \cdot x^2 \bmod m \mid a \in S \}$ .

Zu zeigen:  $H_1$  ist nicht  $c$ -universal.

Seien  $x, y$  2 Schlüssel. Es gilt:

$$h(x) = a \cdot x^2 \bmod m$$

$$h(y) = a \cdot y^2 \bmod m$$

$$(ax^2 = ay^2) \bmod m$$

Nach der Definition gilt  $x \neq y$

$$\Rightarrow (ax^2 = ay^2) \bmod m \Leftrightarrow a(x^2 - y^2) = 0 \pmod{m}$$

Da  $m$  keine Primzahl ist, können wir nicht garantieren, dass diese Gleichung nur eine Lösung hat

$$\Rightarrow P(h(x) = h(y)) \neq \frac{1}{m} \Rightarrow H_1 \text{ ist } c\text{-universell.}$$

*(???)*

b) Seien  $x, y$  2 Schlüssel. Es gilt:

Da  $x \neq y$  gilt, gilt  $x_i \neq y_i$  für mind. ein  $i \in \{0, \dots, k\}$ .

$$\text{Wir definieren } h(x) := \sum_{i=0}^k a_i x_i \bmod m \quad \text{und} \quad h(y) := \sum_{i=0}^k a_i y_i \bmod m$$

Wir suchen  $P(h(x) = h(y))$

$$\Rightarrow \sum_{i=0}^k a_i x_i = \sum_{i=0}^k a_i y_i \bmod m$$

$$\Rightarrow \sum_{i=0}^k a_i (x_i - y_i) = 0 \pmod{m}$$

$$(*) \Rightarrow a_j (x_j - y_j) = - \sum_{\substack{i=0 \\ i \neq j}}^k a_i (x_i - y_i) \pmod{m}$$

Für jedes  $a_j \in \{1, \dots, m-1\}$  gibt es genau eine Lösung, da  
m eine Primzahl ist und  $x_j - y_j$  besitzt ein inverses  
Element, da  $\mathbb{Z}_m$  ein Körper ist (Weil m prim ist)

$$\Rightarrow P(h(x)=h(y)) = \frac{1}{m} \Rightarrow H_2 \text{ ist } \ell\text{-universell}.$$