



1. (15 Punkte)

Sei  $U = \{0, 1, 2, 3, 4, 5\}$  und  $T = \{0, 1, 2\}$ . Betrachten wir die folgenden 5 Funktionen von  $U$  nach  $T$ :

$$h_1(x) = (x + 1) \bmod 3 \quad h_2(x) = (x + 2) \bmod 3 \quad h_3(x) = x \bmod 2$$

$$h_4(0) = h_4(5) = 2 \quad h_4(1) = h_4(2) = 1 \quad h_4(3) = h_4(4) = 0$$

$$h_5(0) = h_5(1) = 2 \quad h_5(2) = h_5(3) = 1 \quad h_5(4) = h_5(5) = 0$$

Bestimmen Sie eine Funktion  $h_6$  von  $U$  nach  $T$ , sodass  $\{h_1, h_2, h_3, h_4, h_5, h_6\}$  eine universelle Menge von Hashfunktionen bildet.

2. (15 Punkte)

Eine Menge  $\mathcal{H}$  von Funktionen  $h : U \rightarrow \{0, 1, \dots, t-1\}$  heißt *pseudo-universell*, wenn für jedes  $x \in U$  und jedes  $i \in \{0, 1, \dots, t-1\}$  gilt

$$\frac{|\{h \in \mathcal{H} \mid h(x) = i\}|}{|\mathcal{H}|} \leq \frac{1}{t}.$$

Es sei nun  $S \subset U$  mit  $|S| = n$ .

(a) Zeigen Sie, dass bei zufälliger Wahl einer Hashfunktion aus einer pseudo-universellen Familie  $\mathcal{H}$  für jedes  $i \in \{0, 1, \dots, t-1\}$  die erwartete Anzahl von Elementen von  $S$ , die durch  $h$  auf  $i$  abgebildet werden, höchstens  $n/t$  ist. Die erwartete Größe jedes "Hash-buckets" ist also  $n/t$ .

(b) Zeigen Sie, dass trotz der kleinen erwarteten Hash-bucket-Größen pseudo-universelle Hashfunktionen keine gute Idee sind.

Geben Sie eine Familie  $\mathcal{H}$  an, die zwar pseudo-universell ist, für die aber die Operationen SEARCH und DELETE wesentlich mehr als  $\Omega(n/t)$  Operationen brauchen.

3. (10 Punkte)

Es sei  $U$  ein Schlüsseluniversum und für  $i = 0, 1$  sei  $T_i$  jeweils eine Hashtafel der Größe  $t_i$ . Des weiteren seien  $\mathcal{H}_i$  jeweils eine universelle Familie von Hashfunktionen von  $U$  nach  $T_i$ .

Es sei nun  $T = T_0 \times T_1$  eine Hashtafel der Größe  $t = t_0 \cdot t_1$ . Wir können ein Paar  $(h_0, h_1) \in \mathcal{H}_0 \times \mathcal{H}_1$  als Funktion von  $U$  nach  $T$  auffassen, definiert als

$$(h_0, h_1)(x) = (h_0(x), h_1(x)).$$

Zeigen Sie, dass die Familie  $\mathcal{H}$  aller dieser Paare eine universelle Familie von Hashfunktionen von  $U$  nach  $T$  bildet.



4. (15 Punkte)

Es sei  $U = \{0, 1\}^d$  die Menge aller Bitstrings der Länge  $d$ . Für jedes  $a \in U$  definiere die Funktion  $h_a : U \rightarrow \{0, 1\}$  durch

$$h_a(x) = (a_1 \wedge x_1) \text{ xor } (a_2 \wedge x_2) \text{ xor } \dots \text{ xor } (a_d \wedge x_d).$$

- (a) Zeigen Sie, dass die Menge  $\mathcal{H} = \{h_a | a \in U\}$  eine universelle Menge von Funktionen von  $U$  nach  $\{0, 1\}$  ist.
- (b) Wie kann man mit dieser Idee eine universelle Familie von Hashfunktionen von  $U$  nach  $\{0, 1\}^s$  bekommen für irgendein gegebenes  $s > 1$ ?