

Übungsblatt 11

Aufgabe 1. In dieser Aufgabe soll eine alternative Klasse von Fingerprint-Funktionen betrachtet werden. Für ein Wort $w = a_1 \dots a_n \in \{0, 1\}^*$ definiere

$$h(a_1 \dots a_n) = \sum_{i=1}^n a_i 2^{n-i}.$$

Sei $h_p(w) = h(w) \bmod p$ der *Fingerprint* von w bzgl. einer Primzahl p .

- (a) Entwerfen Sie einen randomisierten Pattern-Matching-Algorithmus mit Hilfe der obigen Fingerprint-Funktionen.
- (b) Wie hoch ist die Wahrscheinlichkeit, dass Ihr Algorithmus einen ungültigen Match liefert?

Aufgabe 2. Alice und Bob besitzen jeweils n -Bit-Dateien $a_1 \dots a_n$ und $b_1 \dots b_n$, und möchten überprüfen, ob sie identisch sind. Dazu einigen sie sich auf eine Primzahl $p > 1000n$ und wählen zufällig eine Zahl $x \in \{0, \dots, p-1\}$ aus. Alice berechnet

$$A(x) = \left(\sum_{i=1}^n a_i x^{n-i} \right) \bmod p$$

und analog berechnet Bob $B(x)$. Wie groß ist die Wahrscheinlichkeit, dass $A(x) = B(x)$ gilt, obwohl die Dateien verschieden sind?

Aufgabe 3. Seien $X = (x_1, \dots, x_m)$ und $Y = (y_1, \dots, y_n)$ Folgen. Nenne X *Teilfolge* von Y , wenn Indizes $1 \leq i_1 < i_2 < \dots < i_k \leq n$ existieren, so dass für alle $1 \leq j \leq k$ gilt $x_j = y_{i_j}$.

Lösen Sie das folgende Problem effizient mit dynamischer Programmierung: Gegeben zwei Folgen X, Y , was ist die maximale Länge einer Folge Z , die Teilfolge von X und Y ist?