

Willkommen zur vierten Saalübung

## Aufgabe 3.1

Es sei  $A$  ein Alphabet.

a) Schreiben Sie einen Algorithmus auf, der folgendes leistet:

- Als Eingaben erhält er ein Wort  $w : \mathbb{G}_n \rightarrow A$  und zwei Symbole  $x \in A$  und  $y \in A$ .
- Am Ende soll eine Variable  $r$  den Wert 0 oder 1 haben, und zwar soll gelten:

$$r = \begin{cases} 1 & \text{falls irgendwo in } w \text{ direkt hintereinander} \\ & \text{erst } x \text{ und dann } y \text{ vorkommen} \\ 0 & \text{sonst} \end{cases}$$

## Aufgabe 3.1

b) Schreiben Sie logische Formeln (mit Quantor(en)) auf, die die folgende Formulierung formalisiert:

„Irgendwo in  $w$  kommen direkt hintereinander erst  $x$  und dann  $y$  vor.“

## Aufgabe 3.1

c) Geben Sie eine Schleifeninvariante an, die nichttrivial ist und den „wesentlichen Aspekt“ Ihres Algorithmus widerspiegelt.

## Aufgabe 3.2

Gegeben ist der folgende Algorithmus. Es sei  $\mathbb{N}_+ = \mathbb{N}_0 \setminus \{0\}$ :

Eingaben:  $a \in \mathbb{N}_+, b \in \mathbb{N}_+$

$X_0 \leftarrow a$

$Y_0 \leftarrow b$

$P_0 \leftarrow 1$

$x_0 \leftarrow X_0 \bmod 2$

$n \leftarrow 1 + \lceil \log_2 a \rceil$

**for**  $i \leftarrow 0$  **to**  $n - 1$  **do**

$P_{i+1} \leftarrow P_i \cdot Y_i^{x_i}$

$X_{i+1} \leftarrow X_i \text{ div } 2$

$Y_{i+1} \leftarrow Y_i^2$

$x_{i+1} \leftarrow X_{i+1} \bmod 2$

## Aufgabe 3.2

- a) Welchen Wert hat am Ende die Variable  $P_n$ ?
- b) Geben Sie für  $i \in \mathbb{N}_0$  Aussagen  $\mathcal{A}_i$  an.  $\mathcal{A}_i$  soll eine Aussage über die Werte der Variablen  $P_i$ , usw nach  $i$  Schleifendurchläufen machen, die „das Wesentliche“ des Algorithmus widerspiegelt.
- c) Beweisen Sie  $\forall i \in \mathbb{N}_0 : \mathcal{A}_i$ .

## Aufgabe 3.2

**for**  $i \leftarrow 0$  **to**  $n - 1$  **do**

$$P_{i+1} \leftarrow P_i \cdot Y_i^{x_i}$$

$$X_{i+1} \leftarrow X_i \text{ div } 2$$

$$Y_{i+1} \leftarrow Y_i^2$$

$$x_{i+1} \leftarrow X_{i+1} \text{ mod } 2$$

Induktionsannahme: Es gibt ein  $i \in \mathbb{N}_0$ , für das gilt:

$$P_i \cdot X_i^{Y_i} = b^a.$$

## Aufgabe 3.2

d) Was passiert, wenn man im Algorithmus  $\lfloor \log_2 a \rfloor$  statt  $\lceil \log_2 a \rceil$  schreibt? Begründung?