Übungsblatt 5

Kufleitner
FMI/TI
Universität Stuttgart

Abgabe der schriftlichen Aufgabe bis Sonntag, den 17. Dezember, 23:59 Uhr.

Aufgabe 1: Pattern-Matching

Teil des Algorithmus von Knuth-Morris-Pratt ist die Funktion BerechneTabelle. *Zur Erinnerung:* Auf Eingabe eines Arrays $P[1 \dots m]$ gibt diese Funktion ein Array $S[1 \dots m]$ aus, sodass für $1 \leqslant q \leqslant m$ gilt:

$$S[q] = \max\bigl\{k < q \mid P[1 \dots k] = P[q-k+1 \dots q]\bigr\}.$$

Führen Sie die Funktion BerechneTabelle mit der Eingabe $P[1 \dots 6] = aabaab$ aus; dokumentieren Sie den Ablauf und insbesondere jeden Vergleich von Buchstaben.

Aufgabe 2: Verknüpfungstafeln

(a) Geben Sie die Verknüpfungstafeln von $(\mathbb{Z}/6\mathbb{Z}, +)$ und $(\mathbb{Z}/6\mathbb{Z}, \cdot\,)$ an. Bestimmen Sie die neutralen Elemente sowie die Inversen der invertierbaren Elemente.

(b) Finden Sie einen Körper $(\mathbb{F}_4, +, \cdot\,)$ mit 4 Elementen, indem Sie auf geeignete Weise die Verknüpfungstafeln $(\mathbb{F}_4, +)$ und $(\mathbb{F}_4, \cdot\,)$ konstruieren.

Aufgabe 3: Kongruenzen in Monoiden

Sei $(M, \circ)$ ein Monoid. Eine Äquivalenzrelation $\sim$ auf M ist eine *Kongruenz*, wenn

$$x \sim x' \wedge y \sim y' \implies x \circ y \sim x' \circ y'$$

für alle $x, x', y, y' \in M$ gilt. Wir bezeichnen im Folgenden mit $[x]$ die *Äquivalenzklasse* von $x \in M$ bezüglich $\sim$ und mit $M/\!\sim$ die zugehörige *Quotientenmenge*, das heißt:

$$[x] := \{x' \in M \mid x \sim x'\} \quad \text{und} \quad M/\!\sim := \{[x] \mid x \in M\}.$$

(a) Zeigen Sie: Ist $\sim$ eine Kongruenz auf $(M, \circ)$, so ist durch

$$\circ\colon M/\!\sim \times M/\!\sim \to M/\!\sim \quad \text{mit} \quad [x] \circ [y] = [x \circ y]$$

eine Verknüpfung auf $M/\!\sim$ definiert, sodass $(M/\!\sim, \circ)$ wieder ein Monoid ist.

Wir betrachten nun auf dem Monoid $(\mathbb{N} \times \mathbb{N}, +)$ mit komponentenweiser Addition

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

eine Relation $\sim$. Diese ist für $(x_1, x_2), (x_1', x_2') \in \mathbb{N} \times \mathbb{N}$ definiert durch

$$(x_1, x_2) \sim (x_1', x_2') \iff x_1 + x_2' = x_1' + x_2.$$

(b) Zeigen Sie, dass $\sim$ eine Kongruenz auf $(\mathbb{N} \times \mathbb{N}, +)$ ist. Finden Sie außerdem einen Isomorphismus zwischen dem Quotientenmonoid $(\mathbb{N} \times \mathbb{N}/\!\sim, +)$ und $(\mathbb{Z}, +)$.

Aufgabe 4: Euklid's Algorithmus

Berechnen Sie jeweils mit dem Euklidischen Algorithmus den größten gemeinsamen Teiler $\mathrm{ggT}(x, y)$ sowie ganze Zahlen p und q mit $px + qy = \mathrm{ggT}(x, y)$:

(a) $x = 44, y = 126$ (b) $x = 33, y = 117$ (c) $x = 19, y = 98$ (d) $x = 27, y = 113$.

Aufgabe 5: Modulare Arithmetik (schriftlich, 10 Punkte)

Zwei Zahlen $x, y \in \mathbb{Z}$ heißen *kongruent modulo* n, für eine natürliche Zahl n, falls eine Zahl $q \in \mathbb{Z}$ existiert, sodass $x = y + qn$ gilt. Wir schreiben dann $x \equiv y \pmod{n}$.

(a) (3 Punkte) Zeigen Sie für alle $x, y, z \in \mathbb{Z}$ und $n \in \mathbb{N}$:

$$x \equiv y \pmod{n} \implies x + z \equiv y + z \pmod{n}.$$

Gilt auch die Gegenrichtung der Implikation? Beweisen Sie Ihre Antwort.
Folgern sie außerdem hieraus für alle $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ und $n \in \mathbb{N}$:

$$x_1 \equiv y_1 \pmod{n} \land x_2 \equiv y_2 \pmod{n} \implies x_1 + x_2 \equiv y_1 + y_2 \pmod{n}.$$

(b) (3 Punkte) Zeigen Sie für alle $x, y, z \in \mathbb{Z}$ und $n \in \mathbb{N}$:

$$x \equiv y \pmod{n} \implies xz \equiv yz \pmod{n}.$$

Gilt auch die Gegenrichtung der Implikation? Beweisen Sie Ihre Antwort.
Folgern sie außerdem hieraus für alle $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ und $n \in \mathbb{N}$:

$$x_1 \equiv y_1 \pmod{n} \land x_2 \equiv y_2 \pmod{n} \implies x_1 x_2 \equiv y_1 y_2 \pmod{n}.$$

(c) (2 Punkte) Zeigen Sie für alle $x, y \in \mathbb{Z}$ und $m, n \in \mathbb{N}$:

$$x \equiv y \pmod{mn} \implies x \equiv y \pmod{m} \land x \equiv y \pmod{n}.$$

Gilt auch die Gegenrichtung der Implikation? Beweisen Sie Ihre Antwort.

(d) (2 Punkte) Zeigen Sie für alle $x, y \in \mathbb{Z}$ und teilerfremden $m, n \in \mathbb{N}$:

$$x \equiv y \pmod{m} \land x \equiv y \pmod{n} \implies x \equiv y \pmod{mn}.$$

Hinweis: Verwenden Sie das Lemma von Bézout.

Aufgabe 6: Transitionsmonoide

Sei $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$ ein deterministischer endlicher Automat. Die Elemente des zugehörigen *Transitionsmonoids* $T_\mathcal{A}$ sind die Funktionen

$$\begin{aligned} \delta_w : Q &\longrightarrow Q \\ q &\longmapsto \delta(q, w) \end{aligned}$$

für $w \in \Sigma^*$. Die Verknüpfung $\bullet$ von $T_\mathcal{A}$ ist die umgekehrte[1] Funktionenkomposition. Diese ist durch $(\delta_u \bullet \delta_v)(q) = (\delta_v \circ \delta_u)(q) = \delta_v(\delta_u(q))$ definiert. Es gilt $\delta_u \bullet \delta_v = \delta_{uv}$.

(a) Zeigen Sie, dass das Transitionsmonoid $T_\mathcal{A}$ ist genau dann eine Gruppe ist, wenn der Automat $\mathcal{A}$ co-deterministisch ist, d. h. wenn für alle $p, q \in Q$ und $a \in \Sigma$ gilt:

$$\delta(p, a) = \delta(q, a) \implies p = q.$$

Eine Sprache $L \subseteq \Sigma^*$ wird durch ein endliches Monoid M *erkannt*, wenn ein Monoid-Homomorphismus $\varphi\colon \Sigma^* \to M$ existiert, sodass $L = \varphi^{-1}(N)$ für ein $N \subseteq M$ gilt.

(b) Zeigen Sie, dass die Sprache $L(\mathcal{A})$ vom Transitionsmonoid $T_\mathcal{A}$ erkannt wird.

[1] Wir lesen Wörter von links nach recht, werten Funktionen aber von rechts nach links aus. Um diese Aktivitäten in Beziehung zu setzten, ist es hier hilfreich, eine dieser Richtungen formal umzukehren.