Logik und diskrete Strukturen
Wintersemester 2015/16

Abgabe: Keine Abgabe

universitätbonn

Prof. Dr. Heiko Röglin
Anna Großwendt
Clemens Rösner
Institut für Informatik

Übungsblatt 13

Aufgabe 13.1

(a) Zeigen Sie mithilfe eines Widerspruchsbeweises, dass es unendlich viele natürliche Zahlen gibt, die durch 3 teilbar sind.

(b) Es bezeichne $P \subseteq \mathbb{N}$ die Menge aller Primzahlen. Wir definieren eine Relation R auf der Menge $\mathbb{N}$ wie folgt: Für $n_1, n_2 \in \mathbb{N}$ gelte $(n_1, n_2) \in R$ genau dann, wenn $\{x \in P \mid x \text{ teilt } n_1\} = \{x \in P \mid x \text{ teilt } n_2\}$. Bestimmen Sie mit Begründung, ob es sich bei R um eine Äquivalenzrelation handelt.

(c) Es sei $X = \{A, B, C, D\}$ und es sei $R = \{(A, C), (C, D), (D, B), (B, D), (C, C)\}$ eine Relation auf X. Bestimmen Sie die kleinste Äquivalenzrelation $Q \supseteq R$.

(d) Es sei $N = \{1, \ldots, n\}$ für ein $n \geq 2$. Wie viele Permutationen π von N mit $\pi(1) \leq 2$ gibt es?

Aufgabe 13.2

(a) Geben Sie einen DFA an, der die folgende Sprache entscheidet:

$$L_1 = \{w \in \{0,1\}^* \mid \text{die Anzahl der 1en oder die Anzahl der 0en in } w \text{ ist ungerade}\}.$$

(b) Seien $L_2 \subseteq \{0,1\}^*$ und $L_3 \subseteq \{0,1\}^*$ reguläre Sprachen. Zeigen Sie, dass dann auch die folgende Sprache regulär ist:

$$L_2 \oplus L_3 = \{w \in \{0,1\}^* \mid w \text{ ist in genau einer der beiden Sprachen } L_2 \text{ und } L_3 \text{ enthalten}\}.$$

(c) Zeigen Sie ohne Verwendung des Pumping-Lemmas, dass es keinen DFA gibt, der die folgende Sprache entscheidet:

$$L_4 = \{0^n 1^{2n} \mid n \in \mathbb{N}\} \subseteq \{0,1\}^*.$$

(d) Zeigen Sie, dass die Nerode-Relation R_{L_4} unendlich viele Äquivalenzklassen besitzt.

(e) Geben Sie einen NFA mit einem akzeptierenden Zustand an, der die folgende Sprache entscheidet:

$$L_5 = \{w \in \{0,1\}^* \mid \text{das vorletzte Zeichen in } w \text{ ist eine 1}\}.$$

(f) Zeigen Sie, dass es keinen DFA mit nur einem akzeptierenden Zustand gibt, der L_5 entscheidet.

(g) Formen Sie den NFA aus Aufgabenteil (f) mittels Potenzmengenkonstruktion in einen DFA um.

(h) Geben Sie einen DFA mit 4 Zuständen an, der L_5 entscheidet, und zeigen Sie, dass dieser minimal ist.

Aufgabe 13.3

(a) Bestimmen Sie mithilfe des euklidischen Algorithmus den größten gemeinsamen Teiler von 13 und 3.

(b) Bestimmen Sie das Inverse von $[\![3]\!]_{13}$ in $(\mathbb{Z}/13\mathbb{Z}, \odot_{13})$.

(c) Bestimmen Sie mithilfe des chinesischen Restsatzes eine Zahl $x \in \{0, \ldots, 38\}$ mit $x \equiv 4 \bmod 3$ und $x \equiv 2 \bmod 13$.

(d) Sie erhalten eine Nachricht $m^e = 3$, welche mit dem RSA-Algorithmus verschlüsselt wurde. Der öffentliche Schlüssel ist $(n, e) = (21, 11)$. Berechnen Sie die ursprüngliche Nachricht m.

(e) Sei $n \in \mathbb{N}$. Zeigen Sie, dass jedes Element $[\![a]\!]_n$ mit $\mathrm{ggT}(a, n) = 1$ in $(\mathbb{Z}/n\mathbb{Z}, \odot_n)$ invertierbar ist.

Aufgabe 13.4

(a) Sei $\varphi = (x_1 \vee x_2) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_1 \vee x_3) \wedge (x_2 \vee \neg x_3) \wedge (\neg x_2 \vee \neg x_3)$. Zeigen Sie mithilfe des Resolutionskalküls, dass φ unerfüllbar ist.

(b) Zeigen Sie mittels struktureller Induktion, dass jede Formel $\varphi \in \mathrm{AL}$ die gleiche Anzahl an öffnenden und schließenden Klammern enthält.

(c) Es sei $\sigma = \{f, g, R, c\}$ eine Signatur mit den Funktionssymbolen f und g, dem Relationssymbol R und dem Konstantensymbol c. Es gelte $\mathrm{ar}(R) = 2$, $\mathrm{ar}(f) = 3$ und $\mathrm{ar}(g) = 2$. Geben Sie eine prädikatenlogische Formel $\varphi \in \mathrm{FO}(\sigma)$ an, in der jedes Symbol aus σ sowie jeder der beiden Quantoren mindestens einmal vorkommt.