Logik und diskrete Strukturen WS 2014/15
Übungsblatt 11
Universität Bonn, Institut für Informatik I

Abgabe: **Donnerstag** 8.1.2014, bis 10:15 Uhr Besprechung: KW 04

- *Die Lösungen können bis zum Abgabetermin in den Postkasten im AVZ III eingeworfen werden (vom Haupteingang in dem kleinen Raum auf der linken Seite). Geben Sie bitte immer gut sichtbar auf dem Deckblatt die Übungsgruppennummer an.*
- *Die Abgabe in festen Gruppen bis zu 3 Personen ist erlaubt, sofern alle in der gleichen Übungsgruppe sind.*

Aufgabe 1: RSA — 4 Punkte

Verschlüsseln Sie den Vornamen eines Mitglieds Ihrer Abgabegruppe mittels RSA mit den Parametern $p = 5$ und $q = 7$. Verwenden Sie dabei die Zeichenkodierung aus dem Beispiel am Ende von Abschnitt 4.3.5 des Vorlesungsskriptes und geben Sie alle durchgeführten Rechenschritte sowie das öffentliche und das private Schlüsselpaar an.

Aufgabe 2: Normalformen — 2+2 Punkte

Sei $\varphi = \big((x_1 \to \neg\, x_2) \wedge \neg(x_3 \leftrightarrow x_1)\big)$.

a) Bestimmen Sie anhand einer Wahrheitstafel eine zu φ äquivalente aussagenlogische Formel in disjunktiver Normalform.

b) Bestimmen Sie mit Hilfe des ErzeugeKNF-Algorithmus aus der Vorlesung eine zu φ äquivalente aussagenlogische Formel in konjunktiver Normalform.

Aufgabe 3: Koinzidenzlemma — 4 Punkte

Zeigen Sie mittels struktureller Induktion: Es sei $\varphi \in AL$ eine Formel und es seien B und B' zwei zu φ passende Bewertungen, sodass $B(x) = B'(x)$ für alle $x \in Var(\varphi)$ gilt. Dann gilt $[\![\varphi]\!]_B = [\![\varphi]\!]_{B'}$.

Aufgabe 4: Gruppen 4 Punkte

Seien $(M, \circ)$ eine Halbgruppe und $e \in M$ ein Element von M mit der Eigenschaft, dass $e \circ x = x$ für alle $x \in M$ gilt und für jedes $y \in M$ ein $x \in M$ mit $x \circ y = e$ existiert. Zeigen Sie, dass $(M, \circ)$ eine Gruppe ist.

Aufgabe 5: Wohldefiniertheit 4 Zusatzpunkte

Betrachten Sie die Menge $K = \{x \in \mathbb{R} \mid \forall q \in \mathbb{Q} : x \cdot q \notin \{\pi, \frac{1}{\pi}\}\} \subseteq \mathbb{R}$ mit der Addition und Multiplikation aus $\mathbb{R}$. Zeigen oder widerlegen Sie, dass $(K, +, \cdot)$ ein Körper ist.

Aufgabe 6: DFAs 3+2+3 Zusatzpunkte

a) Seien $k \in \mathbb{N}$ eine (feste) Zahl und $L \subseteq \{0,1\}^k$ eine Sprache über dem Alphabet $\{0,1\}$. Zeigen Sie, dass es einen DFA M gibt, der L entscheidet und höchstens einen akzeptierenden Zustand besitzt.

b) Geben Sie eine feste Zahl $k \in \mathbb{N}$ und eine reguläre Sprache $L \subseteq \{0,1\}^*$ an, die nur Wörter der Länge höchstens k enthält, sodass kein DFA mit höchstens einem akzeptierenden Zustand existiert, der L entscheidet.

c) Zeigen Sie, dass Ihr Beispiel aus Aufgabenteil (b) die geforderten Bedingungen erfüllt.

Aufgabe 7: Schubfachprinzip 4 Zusatzpunkte

Seien M eine Menge mit $|M| = 6$ und R eine symmetrische Relation auf M. Zeigen Sie, dass es eine Teilmenge $M' \subseteq M$ mit $|M'| = 3$ gibt, so dass entweder $x \; R \; y$ für alle $x \neq y \in M'$ oder $x \not R \; y$ für alle $x \neq y \in M'$ gilt.