Lehr- und Forschungsgebiet
Mathematische Grundlagen der Informatik
RWTH Aachen
Prof. Dr. E. Grädel, B. Pago

SS 2019

7. Übung Mathematische Logik

Abgabe: bis Dienstag, den 28.05., um 14:00 Uhr im Übungskasten (Informatikzentrum, E1, 1. Stock) oder in der Vorlesung.

Geben Sie bitte Namen, Matrikelnummer und die Übungsgruppe oben rechts an.
Übungen, die mit einem Stern markiert sind, sind Bonusaufgaben.

Aufgabe 1 — 7 Punkte

Bearbeiten Sie den eTest im Moodle-Lernraum[1].

Aufgabe 2 — 5 Punkte

Sei $\mathfrak{A} = (\{0, 1\}, <)$, wobei $<$ die übliche Ordnung auf $\{0, 1\}$ sei.
Sei $\psi = (\neg\exists x(x = x)) \vee \forall x\exists y(x < y)$. Geben Sie das Auswertungsspiel $\mathrm{MC}(\mathfrak{A}, \psi)$ an.
Entscheiden Sie, ob $\mathfrak{A} \models \psi$ gilt, indem Sie eine Gewinnstrategie für die Verifiziererin / den Falsifizierer angeben.

Aufgabe 3 — 3 Punkte

Betrachten Sie die $\mathrm{FO}(\{R\})$-Formel

$$\psi = \forall x\forall z((Rx \vee \exists y\exists v(x = y \wedge x = v)) \wedge \exists w(z \neq w)).$$

Schätzen Sie die Größe des resultierenden Auswertungsspiels in Abhängigkeit von der Strukturgröße ab: Geben Sie die kleinste natürliche Zahl k an, sodass die Anzahl der Knoten des Auswertungsspiels $\mathrm{MC}(\mathfrak{A}, \psi)$ in $O(|A|^k)$ ist, für alle endlichen $\{R\}$-Strukturen $\mathfrak{A}$.

Aufgabe 4 — (3 + 2) + 5 Punkte

Eine τ-Struktur $\mathfrak{A}$ heißt *starr*, wenn ihr einziger Automorphismus die Identität ist.

(a) Sei $\mathfrak{A}$ eine τ-Struktur, in der jedes Element elementar definierbar ist, d.h. für alle $a \in A$ ist die Menge $\{a\}$ in $\mathfrak{A}$ durch eine Formel $\varphi_a(x)$ definierbar. Zeigen Sie, dass $\mathfrak{A}$ starr ist.

Gilt die Umkehrrichtung auch?

(b) Beweisen oder widerlegen Sie, dass die folgenden Strukturen starr sind.

(i) $\mathfrak{Q} = (\mathbb{Q}, +, \cdot)$

(ii) $\mathfrak{N} = (\mathbb{N}, \mathrm{Odd})$, wobei Odd eine einstellige Relation sei, die genau die ungeraden natürlichen Zahlen enthält.

(iii) $\mathfrak{G} = (V, E)$:

$$\begin{tikzcd} 2 \arrow[d] & 1 \arrow[l] \arrow[dl] \\ 3 & \end{tikzcd}$$

(iv) $\mathfrak{Z} = (\mathbb{Z}, +)$, wobei $+$ wie üblich definiert sei.

Aufgabe 5 — 10 Punkte

Beweisen oder widerlegen Sie jeweils, dass die angegebenen Relationen in der gegebenen Struktur elementar definierbar sind.

[1] https://moodle.rwth-aachen.de/course/view.php?id=1662

(a) Die Menge $\mathbb{Q}_{\geq 1}$ in $(\mathbb{Q}, \cdot)$.

(b) Die dreistellige Relation $+$ in $(\mathbb{Z}, <)$, wobei $+ := \{(x, y, z) \mid x, y, z \in \mathbb{Z}, x + y = z\}$.

(c) Die Menge $\{0, 1\}$ in $(\mathbb{Z}/5\mathbb{Z}, +)$.

(d) Die Menge $\{n \in \mathbb{N} \mid n \text{ ist Vielfaches von } 4\}$ in $(\mathbb{N}, +)$.

(e) Die Relation $\{(a, b) : \text{ggt}(a, b) \neq 1\}$ in $(\mathbb{N}, +, \cdot)$.[2]

Aufgabe 6* 15* Punkte

Wir definieren für jedes $n \in \mathbb{N}^{\geq 1}$ die Struktur $\mathfrak{A}_n$ wie folgt:
$\mathfrak{A}_n := (\{0, 1\}^n, E_n)$, wobei $E_n := \{(v, w) \mid v, w \in \{0, 1\}^n, h(v, w) = 1\}$; dabei bezeichne $h(v, w)$ den Hamming-Abstand der $\{0, 1\}$-Wörter v und w, d.h. die Anzahl der Positionen, an denen sich v und w unterscheiden.

Betrachten Sie weiterhin folgende Gruppen:

- Sei $G_n := (\{0, 1\}^n, \oplus)$, d.h. die Menge der n-stelligen $\{0, 1\}$-Wörter mit der positionsweisen XOR-Verknüpfung (also z.B. ist $001 \oplus 101 = 100$).
- Sei $H_n := (S_n, \circ)$, also die symmetrische Gruppe, die aus allen Permutationen einer n-elementigen Menge mit der Komposition $\circ$ als Verknüpfung besteht.
- Wir definieren eine neue Gruppe als das Produkt dieser Gruppen: $G_n \times H_n := (\{0, 1\}^n \times S_n, \circ)$, wobei wir die Gruppenverknüpfung $\circ$ wie folgt definieren: Seien $(v, \pi), (v', \pi') \in \{0, 1\}^n \times S_n$. Dann ist $(v, \pi) \circ (v', \pi') := (v \oplus \pi(v'), \pi \circ \pi')$, wobei $\pi(v') := v'_{\pi(1)} v'_{\pi(2)} \dots v'_{\pi(n)}$, d.h. π angewandt auf ein Wort v' ist einfach das Wort, das man erhält, indem man die Positionen von v' entsprechend π vertauscht.

In dieser Aufgabe soll gezeigt werden, dass für alle n die Automorphismengruppe $\text{Aut}(\mathfrak{A}_n)$ isomorph ist zu $G_n \times H_n$.

(a) Geben Sie eine Abbildung $f : G_n \times H_n \to \text{Aut}(\mathfrak{A}_n)$ an, die injektiv ist und verträglich mit den Gruppenoperationen, d.h. es muss gelten: $f((v, \pi) \circ (v', \pi')) = f(v, \pi) \circ f(v', \pi')$ für alle $(v, \pi), (v', \pi') \in G_n \times H_n$. Beweisen Sie, dass Ihr f diese Eigenschaften hat; denken Sie insbesondere daran, zu beweisen, dass $f(v, \pi)$ auch wirklich immer ein Automorphismus von $\mathfrak{A}_n$ ist. Kurz gesagt: Überlegen Sie sich, auf welche Weise jedes Paar aus einem Wort in $\{0, 1\}^n$ und einer Permutation von n Elementen einen Automorphismus von $\mathfrak{A}_n$ beschreibt.

(b) Zeigen Sie, dass die Abbildung f aus (a) auch surjektiv ist. Betrachten Sie dazu einen beliebigen Automorphismus $\rho \in \text{Aut}(\mathfrak{A}_n)$. Zeigen Sie, dass ρ bereits eindeutig festgelegt ist, wenn $\rho(000\dots0000)$, $\rho(000\dots0001)$, $\rho(000\dots0010)$, ..., $\rho(100\dots0000)$ (d.h. das Bild von jedem Wort mit keiner oder einer 1) gegeben sind: Dazu können Sie Induktion führen über die Anzahl m der 1en in einem Wort, um zu zeigen, dass $\rho(v)$ eindeutig festgelegt ist für alle $v \in \{0, 1\}^n$ mit m 1en. Folgern Sie, dass ρ ein Urbild unter f hat.

[2] $\text{ggt}(a, b)$ bezeichnet den größten gemeinsamen Teiler von a und b.