Logik und diskrete Strukturen
Wintersemester 2017/18

Abgabe: 16.01.18 - 10:15
Besprechung: 22.01.2018 - 26.01.2018

UNIVERSITÄT BONN

Prof. Dr. Rolf Klein
Barbara Schwarzwald
Institut für Informatik

Übungszettel 11

Aufgabe 11.1: Euklidischer Algorithmus (4 Punkte)

Der euklidische Algorithmus aus der Vorlesung durchläuft eine while-Schleife solange, bis b gleich 0 ist. Sei die Folge der Fibonacci-Zahlen f_n durch folgende Rekursion definiert:

$$f_0 = 0, f_1 = 1 \text{ und für alle } n \geq 0 : f_{n+2} = f_n + f_{n+1}.$$

Beweisen Sie, dass für jedes $k \geq 2$ gilt: Der euklidische Algorithmus durchläuft die while-Schleife genau $(k-1)$-mal, wenn er auf das Zahlenpaar (f_{k+1}, f_k) angewandt wird.

Aufgabe 11.2: RSA Verschlüsselung (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 11.3: Strukturelle Induktion über Aussagen (4 Punkte)

Sei φ eine aussagenlogische Formel. Zeigen Sie mittels struktureller Induktion, dass die Ungleichung

$$\sum_{i \in \mathbb{N}} |\varphi|_{x_i} \leq |\varphi|_(+ 1$$

gilt. Dabei gibt $|\varphi|_a$ an, wie oft das Zeichen a in der Formel φ enthalten ist.

Aufgabe 11.4: Bewertung von Aussagen (4 Punkte)

a) Entscheiden Sie für die folgenden Formeln, ob sie jeweils erfüllbar, gültig oder unerfüllbar sind.

- $\Big(x_2 \vee \big((x_1 \wedge x_2) \to x_3\big)\Big)$
- $\big((x_1 \to x_2) \leftrightarrow (\neg x_2 \to \neg x_1)\big)$
- $\Big((x_1 \to x_2) \leftrightarrow \big((x_1 \wedge \neg x_2) \to \mathbf{0}\big)\Big)$

b) Wir betrachten die aussagenlogischen Formeln φ_n, gegeben durch

$$\varphi_n = \begin{cases} (x_n \leftrightarrow x_{n+2}) & \text{falls } n \text{ gerade}, \\ (x_n \leftrightarrow \neg x_{n-1}) & \text{falls } n \text{ ungerade}, \end{cases}$$

für alle $n \in \mathbb{N}$. Geben Sie eine Bewertung an, die φ_n für alle $n \in \mathbb{N}$ erfüllt.