Übungen zur Vorlesung Entscheidungsverfahren mit Anwendungen in der Softwareverifikation | Wintersemester 2018/19 | Aufgabenblatt 6

Institut für Theoretische Informatik, Karlsruher Institut für Technologie (KIT)
Prof. Dr. Carsten Sinz

30.01.2019
Abgabe: 12.02.2019

Aufgabe 18 (algebraische Körpererweiterungen) [5 Punkte]

Betrachten Sie die algebraischen Körpererweiterungen $L = \mathbb{Q}(\sqrt{3}+\sqrt{5})$ und $L' = \mathbb{Q}(\sqrt{3},\sqrt{5})$. L' ist der kleinste Erweiterungskörper von $\mathbb{Q}$, der sowohl $\sqrt{3}$ als auch $\sqrt{5}$ enthält. Zeigen Sie: $L = L'$.

Hinweise: Das Minimalpolynom von $\alpha = \sqrt{3}+\sqrt{5}$ über $\mathbb{Q}$ ist $m_\alpha(x) = x^4 - 16x^2 + 4$. Für $L \supseteq L'$ können Sie zeigen, dass sowohl $\sqrt{3} \in \mathbb{Q}(\alpha)$ als auch $\sqrt{5} \in \mathbb{Q}(\alpha)$, indem Sie diesen Zahlen entsprechende Polynome im Restklassenring $\mathbb{Q}[x]/m_\alpha(x)$ angeben.

Aufgabe 19 (Sturm-Sequenz) [5+5 Punkte]

a) Bestimmen Sie für die Polynome

$$p_1(x) = x^5 - 5x^3 + 4x \qquad \text{und}$$
$$p_2(x) = x^4 - x^2 - x - 1$$

die Anzahl deren reeller Nullstellen. Berechnen Sie dazu die Sturm-Sequenz für beide Polynome.

b) Geben Sie für jede Nullstelle auch ein isolierendes Intervall an, d.h. zwei Zahlen $a, b \in \mathbb{Q}$, $a < b$, so dass im halboffenen Intervall $(a, b]$ genau eine Nullstelle liegt.

Aufgabe 20 (quadratfreie Polynome) [5 Punkte]

Ein Polynom p heißt quadratfrei, wenn es kein Polynom b mit Grad ≥ 1 gibt, so dass $b^2 | p$. Zeigen Sie: Ein univariates Polynom p über $\mathbb{Q}$ ist genau dann quadratfrei, wenn $\mathtt{ggT}(p, p') = 1$, wobei p' die Ableitung von p bezeichnet.

Hinweis: Der Polynom-ggT g ist nicht eindeutig, da die Multiplikation von g mit einer Zahl $c \in \mathbb{Q}$ ebenfalls ein ggT ist. In dieser Aufgabe soll der ggT immer das normierte Polynom (d.h. Leitkoeffizient 1) sein.

Aufgabe 21 (lineare Quantoren-Elimination) [optional, 10 Punkte]

Geben Sie ein Verfahren zur Quantoren-Elimination an, das für lineare Arithmetik über den rationalen Zahlen geeignet ist. Dabei sollen die atomaren Formeln die Gestalt

$$\sum_{i=1}^{n} a_i \cdot x_i \odot 0 \quad \text{mit } \odot \in \{=, <, >\}$$

mit Koeffizienten $a_i \in \mathbb{Q}$ und Unbekannten x_i besitzen.

Wichtiger Hinweis: Da die Abgabe der Lösungen noch bis in die erste Semesterferienwoche erfolgen kann, müssen die Ausarbeitungen für dieses Blatt schriftlich abgegeben werden (in Raum 028). Die korrigierten und bewerteten Aufgabenblätter können dann am 15.02. in der Sprechstunde abgeholt werden.