Prof. Dr. M. Grohe
E. Fluck, A. Riazsadri, J. Feith

Übungsblatt 7 mit Lösungen

Abgabetermin: Mittwoch, der 7. Dezember 2022 um 14:30

Aufgabe 4 (Loop-Berechenbarkeit) **5 Punkte**

Zeigen Sie, dass folgende arithmetische Befehle LOOP-berechenbar sind:

a) $x_i := x_j$ DIV x_k (Division ohne Rest, gegeben $x_k > 0$),

b) $x_i := x_j$ MOD x_k (Modulo, gegeben $x_k > 0$).

Lösung:

a) Wir suchen das kleinste $x_i \leq x_j$ so dass $(x_i + 1) \cdot x_k > x_j$. Dazu probieren wir alle x_i von 0 bis x_j aus.

Daher, falls wir ein x_i mit $(x_j + 1) - (x_i \cdot x_k) \leq 0$ finden, ist das Ergebnis $(x_i - 1)$. Wir beginnen daher mit $x_i = 1$ und dem Test von $d := (x_j + 1) - x_k = 0$. Für nachfolgende Werte von x_i, können wir d um x_k vermindern.

$x_i := 1;$
$d := x_j + 1;$
$d := d \dot{-} x_k;$
LOOP x_j DO
    IF $d = 0$ THEN $x_i := x_i$ ELSE
        $x_i := x_i + 1;$
        $d := d \dot{-} x_k;$
    ENDIF
ENDLOOP;
$x_i := x_i \dot{-} 1$

Es genügen x_j Iterationen der LOOP-Schleife, da $(x_j + 1) \cdot x_k > x_j$ gilt. Im Fall $x_k = 1$ ist diese Anzahl auch tatsächlich notwendig.

b) Wir benutzen, dass wir in (a) gezeigt haben, dass es ein LOOP-Programm gibt, das die Division ohne Rest berechnet. Zudem ist nach Vorlesung die Multiplikation LOOP-berechenbar und nach Tutoraufgabe 7.1 (b) auch die Subtraktion.

$y := x_j$ DIV $x_k;$
$y := y \cdot x_k;$
$x_i := x_j \dot{-} y$

Aufgabe 5 (Monotonie der Ackermannfunktion) **5 Punkte**

Zeigen Sie, dass $A(m, n+1) > A(m, n)$ für alle $m, n \in \mathbb{N}$ gilt. Sie dürfen dabei ohne Beweis verwenden, dass $A(m+1, n) > A(m, n)$ für alle $m, n \in \mathbb{N}$ gilt.

Lösung:

Wir beweisen die Aussage mittels Induktion. **I.A.:** Nach Definition gilt für alle $n \in \mathbb{N}$, dass $A(0, n+1) = n+1 > n = A(0, n)$

I.V.: Für alle $n \in \mathbb{N}$ und ein beliebig aber festes $m_0 \in \mathbb{N}$ gelte

$$A(m_0, n+1) > A(m_0, n). \tag{1}$$

I.S.: Wir zeigen zunächst mittels (verschachtelter) Induktion, dass $A(m_0+1, n+1) > A(m_0+1, n)$ für alle $n \in \mathbb{N}$ gilt.

(I.A.2:) Sei $n = 0$, dann gilt laut Vorlesung $A(m_0+1, 1) = A(m_0+2, 0) > A(m_0+1, 0)$.

(I.V.2:) Für ein beliebiges aber festes $n_0 \in \mathbb{N}$ gelte $A(m_0+1, n_0+1) > A(m_0+1, n_0)$.

(I.S.2:) Per Definition gilt, dass $A(m_0+1, n_0+2) = A(m_0, A(m_0+1, n_0+1))$. Unter Nutzung der (zweiten) Induktionsvoraussetzung erhalten wir also $A(m_0+1, n_0+1) > A(m_0+1, n)$. Wir nutzen nun die erste Induktionsvoraussetzung und erhalten so

$$\begin{aligned} A(m_0+1, n_0+2) &= A(m_0, A(m_0+1, n_0+1)) \\ &> A(m_0, A(m_0+1, n_0)) = A(m_0+1, n_0+1). \end{aligned}$$

Somit gilt $A(m_0+1, n+1) > A(m_0+1, n)$ für alle $n \in \mathbb{N}$.

Außerdem ist damit also auch $A(m, n+1) > A(m, n)$ für alle $m, n \in \mathbb{N}$ bewiesen.

Aufgabe 6 (Alternative Charakterisierung von NP) 5 Punkte

Zeigen Sie, dass es für jede Sprache $L \in \mathsf{NP}$ eine NTM N und ein Polynom $p(X)$ gibt, so dass die Länge *aller* Rechenwege von N bei jeder Eingabe der Länge n höchstens $p(n)$ ist.

Lösung:

Sei L eine Sprache mit $L \in \text{NP}$. Diese Sprache wird also durch eine NTM M erkannt, deren worst case Laufzeit $t_M(n)$ durch ein Polynom $q(n)$ beschränkt ist. Wir zeigen die Existenz einer NTM N mit $L(N) = L$, so dass die Länge *aller* Rechenwege von N bei jeder Eingabe der Länge n höchstens $p(n)$, für ein Polynom $p(X)$ ist.
Auf einer Eingabe x simuliert N das Verhalten von M, zählt dabei aber die Anzahl der Rechenschritte mit und verwirft die Eingabe, sobald $q(|x|) + 1$ Schritte simuliert wurden. Dazu konstruieren wir zunächst eine 3-Band-NTM, die sich folgendermaßen verhält:

- Für eine Eingabe x berechnet sie zuerst auf dem zweiten Band $q(|x|)$, was in Polynomialzeit möglich ist.
- Dann arbeitet sie auf dem ersten Band wie M und zählt dabei auf dem dritten Band die Rechenschritte mit.
- Sobald die Schrittanzahl größer ist als die auf dem zweiten Band gespeicherte Zahl, verwirft die Maschine die Eingabe.

Der Laufzeitverlust ist dabei in jedem Schritt höchstens $O(q(|x|))$. Analog zum in der Vorlesung vorgestellten Verfahren kann die 3-Band-NTM in eine (1-Band-)NTM umgewandelt werden, wobei die Länge jedes Rechenwegs nur quadratisch wächst.

Weil die NTM N auf einer Eingabe der Länge n jeden Rechenweg von M nur bis zu einer Länge von $q(n) + 1$ simuliert und dabei nur ein polynomieller Laufzeitverlust entsteht, ist die Länge jedes Rechenweges von N polynomiell beschränkt.

Weiterhin gilt $L(M) = L(N)$:

$$
\begin{aligned}
x \in L(M) &\Leftrightarrow \text{es gibt einen akzeptierenden Rechenweg von } M \text{ auf } x \\
&\Leftrightarrow \text{es gibt einen akzeptierenden Rechenweg von } M \text{ mit Länge} \leq q(|x|) \text{ auf } x \\
&\Leftrightarrow \text{es gibt einen akzeptierenden Rechenweg von } N \text{ auf } x \\
&\Leftrightarrow x \in L(N).
\end{aligned}
$$