Karlsruher Institut für Technologie

Institute of Information Security and Dependability
Dr. Mattias Ulbrich
https://formal.kastel.kit.edu/

Übungsblatt 5

Grundbegriffe der Informatik — Winter 2023/24

Tutor*in:

Tutorium Nr.:

Nach-,Vorname 1: ,

Matr.nr. 1:

Nach-,Vorname 2: ,

Matr.nr. 2:

Ausgabe: 28. November 2023, 14:30 Uhr

Abgabe: 8. Dezember 2023, 12:30 Uhr

Bitte beachten Sie die Hinweise auf der letzten Seite.

---

*Von Tutor*in auszufüllen:*

Blatt 5: / 21

Blätter 1 – 5, Stud. 1: / 101

Blätter 1 – 5, Stud. 2: / 101

Aufgabe 1 - Zeichensalat (4 Punkte)

Gegeben sei das Alphabet $A = \{\texttt{a}, \texttt{b}\}$. Für jede der folgenden Bedingungen B_i mit $i \in \{1, 2, 3, 4\}$ sei $L_i = \{w \in A^* \mid w \text{ erfüllt } B_i\}$ die zugehörige Sprache. Geben Sie für jede Sprache L_i einen formalen Mengenausdruck an, der genau L_i beschreibt. Verwenden Sie hierfür *ausschließlich* folgende Zeichen:

$$\texttt{a} \quad \texttt{b} \quad (\quad) \quad \{ \quad \} \quad , \quad * \quad \cdot \quad \cup$$

a) B_1 = „$|w| = 0$" (1 Punkt)

b) B_2 = „Es kommen je mindestens ein $\texttt{a}$ und $\texttt{b}$ in w vor." (1 Punkt)

c) B_3 = „Das Teilwort $\texttt{ba}$ kommt nicht in w vor." (1 Punkt)

d) B_4 = „Direkt nach jedem $\texttt{a}$ folgen zwei $\texttt{b}$ in w" (1 Punkt)

Lösung 1

a) $L_1 = \{\}^*$

b) $L_2 = \{\texttt{a}, \texttt{b}\}^* \cdot \{\texttt{ab}, \texttt{ba}\} \cdot \{\texttt{a}, \texttt{b}\}^*$

c) $L_3 = \{\texttt{a}\}^* \cdot \{\texttt{b}\}^*$

d) $L_4 = (\{\texttt{b}\}^* \cup \{\texttt{abb}\})^*$

Aufgabe 2 - Geschickt geteilt (3 Punkte)

Zeigen Sie mit Hilfe vollständiger Induktion, dass für alle $n \in \mathbb{N}_+$ die folgende Aussage gilt:

$8^n - 1$ *ist durch 7 teilbar.*

Lösung 2

IA: $n = 1$ Es gilt $8^n - 1 = 8 - 1 = 7$ ist offensichtlich durch 7 teilbar. ✓

IS: $n \rightsquigarrow n + 1$ Sei $n \in \mathbb{N}_+$ fest, aber beliebig.

IV: Es gilt $8^n - 1$ ist durch 7 teilbar.

IB: Es ist zu zeigen, dass $8^{n+1} - 1$ durch 7 teilbar ist.

Es gilt:

$$\begin{aligned} 8^{n+1} - 1 &= 8^{n+1} - 8 + 7 \\ &= 8 \cdot \underbrace{(8^n - 1)}_{\text{durch 7 teilbar nach } \mathbf{IV}} + 7 \end{aligned}$$

Damit ist $8^{n+1} - 1$ durch 7 teilbar. □

Aufgabe 3 - Beweise unter Koffeinmangel (2 Punkte)

Der hinterhältige Dr. Meta hat erneut zugeschlagen! Dieses Mal trifft es die GBI besonders hart, denn Dr. Meta hat ihren gesamten Kaffeevorrat gestohlen. Wie sollen die Agenten denn nun klar denken?

Die Agenten Boole und Kleene haben Wache gestanden und den Schurken sogar ertappt, jedoch nicht die Verfolgung aufgenommen. „Aber warum denn?“, ruft Detektivin Lovelace. „Ihr seid mit euren Fahrrädern doch doppelt so schnell wie er und hättet ihn locker einholen können!“

Boole und Kleene behaupten, ihnen sei sofort klar gewesen, dass sie Dr. Meta nie hätten einholen können. Als sie ihn gesichtet haben, war er schon 100 Meter entfernt. Die Agenten haben die folgende Überlegung angestellt:

Für einen Zeitpunkt $t \in \mathbb{N}_0$ bezeichne $d_{\text{Meta}}(t) \in \mathbb{R}$ die Strecke in Metern, die Dr. Meta zum Zeitpunkt t zurückgelegt hat und $d_{\text{GBI}}(t) \in \mathbb{R}$ die Strecke in Metern, die die Agenten zurückgelegt haben. Die Verfolungsjagd wird mit Hilfe einer unendlichen Folge von Zeitpunkten wie folgt modelliert:

- t_0 = Beginn der Verfolgungsjagd mit $d_{\text{GBI}}(t_0) = 0$ und $d_{\text{Meta}}(t_0) = 100$
- Für jedes $i \in \mathbb{N}_+$ gilt $d_{\text{GBI}}(t_i) = d_{\text{Meta}}(t_{i-1})$.

Intuitiv ist t_i also der Zeitpunkt, zu dem die Agenten an der Stelle ankommen, an der Dr. Meta zum Zeitpunkt t_{i-1} war. Sowohl die Agenten der GBI als auch Dr. Meta bewegen sich jeweils mit konstanter positiver Geschwindigkeit fort, wobei die Agenten doppelt so schnell sind wie Dr. Meta.

Die Behauptung ist nun, dass für alle $n \in \mathbb{N}_0$ gilt, dass $d_{\text{Meta}}(t_n) > d_{\text{GBI}}(t_n)$.

IA: $n = 0$ Es gilt $d_{\text{Meta}}(t_0) = 100 > 0 = d_{\text{GBI}}(t_0)$ ✓

IS: $n \rightsquigarrow n+1$ Sei $n \in \mathbb{N}_0$ fest, aber beliebig.

IV: Die Agenten haben Dr. Meta zum Zeitpunkt t_n noch nicht eingeholt, also $d_{\text{Meta}}(t_n) > d_{\text{GBI}}(t_n)$.

IB: Es ist zu zeigen, dass $d_{Meta}(t_{n+1}) > d_{GBI}(t_{n+1})$.

Es gilt: $d_{\text{GBI}}(t_{n+1}) = d_{\text{Meta}}(t_n) > d_{\text{GBI}}(t_n)$ nach **IV**.

Seien $\Delta_{\text{Meta}} = d_{\text{Meta}}(t_{n+1}) - d_{\text{Meta}}(t_n)$ und $\Delta_{\text{GBI}} = d_{\text{GBI}}(t_{n+1}) - d_{\text{GBI}}(t_n)$. Da die Agenten doppelt so schnell sind wie Dr. Meta, ist $\Delta_{\text{GBI}} = 2 \cdot \Delta_{\text{Meta}}$. Außerdem ist $\Delta_{\text{Meta}} > 0$, denn Dr. Meta bewegt sich nach Voraussetzung mit positiver Geschwindigkeit fort.

$$\begin{aligned} d_{\text{Meta}}(t_{n+1}) &= d_{\text{Meta}}(t_n) + \Delta_{\text{Meta}} \\ &= d_{\text{GBI}}(t_{n+1}) + \Delta_{\text{Meta}} \\ &\overset{\Delta_{\text{Meta}}>0}{>} d_{\text{GBI}}(t_{n+1}) \end{aligned}$$

Also gilt $d_{\text{Meta}}(t_{n+1}) > d_{\text{GBI}}(t_{n+1})$ □

„Also“, folgert Agent Boole, „haben wir schnell eingesehen, dass wir Dr. Meta niemals (in der Zunkunft) hätten einholen können und haben die Verfolgung gar nicht erst aufgenommen.“ Da kann Detektivin Lovelace nur noch mit dem Kopf schütteln. Die Agenten haben sich bei ihrem Versuch, alles induktiv zu modellieren, wohl irgendwo vertan. Analysieren Sie den „Beweis“ von Boole und Kleene und argumentieren Sie, warum dieser fehlerhaft ist.

Lösung 3

Das Problem hier ist, dass die letzte Schlussfolgerung fehlerhaft ist. Die Agenten behaupten, dass sie Dr. Meta nie hätten einholen können, dass also $d_{Meta}(t) > d_{GBI}(t)$ für jeden beliebigen Zeitpunkt, nicht für für jeden Zeitpunkt aus der oben definierten Folge. Das ist allerdings nicht, was mit dieser Induktion gezeigt wurde, denn:

Sei $i \in \mathbb{N}_+$ beliebig und seien $\Delta^i_{Meta} = d_{Meta}(t_i) - d_{Meta}(t_{i-1})$, $\Delta^i_{GBI} = d_{GBI}(t_i) - d_{GBI}(t_{i-1})$. Da die GBI doppelt so schnell ist wie Dr. Meta, gilt $\Delta^i_{GBI} = 2 \cdot \Delta^i_{Meta}$. Also:

$$\begin{aligned} \Delta^i_{Meta} &= d_{Meta}(t_i) - d_{Meta}(t_{i-1}) \\ &= d_{GBI}(t_{i+1}) - d_{GBI}(t_i) \\ &= d_{GBI}(t_i) + \Delta^{i+1}_{GBI} - d_{GBI}(t_i) \\ &= \Delta^{i+1}_{GBI} \\ &= 2 \cdot \Delta^{i+1}_{Meta} \end{aligned}$$

Mit jedem Zeitschritt nimmt die zurückgelegte Strecke also um den Faktor 2 ab. Da Dr. Meta und die GBI sich mit konstanter Geschwindigkeit fortbewegen, folgt daraus, dass auch die Abstände zwischen den Zeitpunkten der oben definierten Folge stets halbiert werden. Damit gibt es eine obere Schranke für die Zeitspanne, die von der Induktion abgedeckt wird:

$$\sum_{i=0} (t_{i+1} - t_i) = \sum_{i=0} \frac{1}{2^i} (t_1 - t_0) = 2(t_1 - t_0)$$

Aufgabe 4 - Starke Induktion (6 Punkte)

In der Vorlesung wurde bereits erwähnt, dass es verschiedene Varianten der vollständige Induktion gibt. Eine solche Variante ist die so genannte *starke Induktion*. Diese funktioniert nach dem folgenden Schema:

Sei $\mathcal{A}(m)$ eine Aussage über $m \in \mathbb{N}_0$. Dann ist $\mathcal{A}$ wahr für alle $n \in \mathbb{N}_0$ mit $n \geq n_0 \in \mathbb{N}_0$ unter den folgenden Annahmen:

- Es gilt $\mathcal{A}_{n_0}$.
- Für alle $n \geq n_0$ gilt: Wenn $\mathcal{A}_k$ für alle $n_0 \leq k \leq n$ gilt, so gilt auch $\mathcal{A}_{n+1}$.

Wir betrachten in dieser Aufgabe die folgende Aussage $\mathcal{A}_n$:
n kann als Summe paarweise verschiedener Zweierpotenzen dargestellt werden.

a) Geben Sie eine solche Summendarstellung für 2; 4; 6; 14 an. (1 Punkt)

b) Beweisen Sie die Aussage $\mathcal{A}_n$ für jede Zahl $n \in \mathbb{N}_0$ mit starker Induktion. (3 Punkte)

Der Name „starke Induktion“ bedeutet nicht, dass starke Induktion ein mächtigeres Werkzeug ist als die vollständige Induktion. Tatsächlich wird in der Vorlesung und im Skript (Abschnitt 6.2) gezeigt, dass jeder Beweis mit starker Induktion in einen mit normaler vollständiger Induktion umgewandelt werden kann.

c) Beweisen Sie die Aussage $\mathcal{A}_n$ für jede Zahl $n \in \mathbb{N}_0$ mit vollständiger Induktion. (2 Punkte)

Lösung 4

a)

$$
\begin{aligned}
Z(2) &= \{1\} \\
Z(4) &= \{2\} \\
Z(6) &= \{1,2\} \\
Z(14) &= \{1,2,3\}
\end{aligned}
$$

b) **IA**: $n = 0$: Die leere Summe, also die Summe von 0 Zweierpotenzen, hat den Wert 0. ✓

IS: $n \rightsquigarrow n+1$ Sei $n \in \mathbb{N}_0$ fest, aber beliebig.

IV: Für alle $k \in \mathbb{N}_0$ mit $k \leq n$ gilt: k kann als Summe von paarweise verschiedenen Zweierpotenzen dargestellt werden.

IB: Es ist zu zeigen, dass sich $n+1$ als Summe paarweise verschiedener Zweierpotenzen dargestellt werden kann.

Sei $i = \max\left\{j \in \mathbb{N}_0 \mid 2^j \leq n+1\right\}$. Dann gilt $n+1 = 2^j + m$, wobei $m \in \mathbb{N}_0$ und $m \leq n$. Außerdem muss $m < 2^i$ sein, denn sonst wäre $n \geq 2 \cdot 2^i = 2^{i+1}$, was im Widerspruch dazu stünde, dass i größtmöglich gewählt wurde.

Wenn $m = 0$, dann ist $n+1 = 2^i$, womit die gesuchte Darstellung von $n+1$ gefunden ist.

Ansonsten lässt sich m nach **IV** als Summe paarweise verschiedener Zweierpotenzen darstellen Sei Z die Menge dieser Zweierpotenzen. Da $2^i > m$ wie oben gezeigt, muss $2^i \notin Z$ gelten.

Damit ist $Z \cup \left\{2^i\right\}$ die Menge der paarweise verschiedenen Zweierpotenzen, deren Summe genau $n+1$ ist. □

c) Zunächst definieren wir für $n \in \mathbb{N}_0$ die Aussage $\mathcal{B}_n$:

Für jedes $i \in \mathbb{N}_0$ mit $i \leq n$ gilt, dass sich i als Summe paarweise verschiedener Zweierpotenzen dargestellt werden kann.

IA: $n = 0$: Die leere Summe, also die Summe von 0 Zweierpotenzen, hat den Wert 0. ✓

IS: $n \rightsquigarrow n+1$ Sei $n \in \mathbb{N}_0$ fest, aber beliebig.

IV: Für alle $k \in \mathbb{N}_0$ mit $k \leq n$ gilt: k kann als Summe von paarweise verschiedenen Zweierpotenzen dargestellt werden.

IB: Es ist zu zeigen, dass alle $k \in \mathbb{N}_+$ mit $k \leq n+1$ gilt: k kann als Summe von paarweise verschiedenen Zweierpotenzen dargestellt werden.

Sei $k \in \mathbb{N}_0$ mit $k \leq n$. Dann kann k nach **IV** als Summe von paarweise verschiedenen Zweierpotenzen dargestellt werden.

Sei $i = \max\left\{j \in \mathbb{N}_0 \mid 2^j \leq n+1\right\}$. Dann gilt $n+1 = 2^j + m$, wobei $m \in \mathbb{N}_0$ und $m \leq n$. Außerdem muss $m < 2^i$ sein, denn sonst wäre $n \geq 2 \cdot 2^i = 2^{i+1}$, was im Widerspruch dazu stünde, dass i größtmöglich gewählt wurde.

Wenn $m = 0$, dann ist $n+1 = 2^i$, womit die gesuchte Darstellung von $n+1$ gefunden ist.

Ansonsten lässt sich m nach **IV** als Summe paarweise verschiedener Zweierpotenzen darstellen Sei Z die Menge dieser Zweierpotenzen. Da $2^i > m$ wie oben gezeigt, muss $2^i \notin Z$ gelten. Damit ist $Z \cup \left\{2^i\right\}$ die Menge der paarweise verschiedenen Zweierpotenzen, deren Summe genau $n+1$ ist.

Also können alle $k' \in \mathbb{N}_0$ mit $k' \leq n+1$ als Summe von paarweise verschiedenen Zweierpotenzen dargestellt werden. $\square$

Aufgabe 5 - Summendarstellung (3 Punkte)

Wir betrachten erneut die Aussage aus der vorherigen Aufgabe. Wir wollen nun eine Funktion $Z : \mathbb{N}_0 \to \mathcal{P}(\mathbb{N}_0)$ angeben, die eine solche Summendarstellung berechnet. Konkret soll für alle $n \in \mathbb{N}_0$ gelten, dass $n = \sum_{k \in Z(n)} 2^k$ (die Summierung über alle Elemente von $Z(n)$, geschrieben als $\sum_{k \in Z(n)}$, ist wohldefiniert, so lange $Z(n)$ endlich ist). $Z(n)$ soll also die Menge aller Exponenten der Zweierpotenzen sein, die aufsummiert n ergeben.

Geben Sie eine Definition für Z an.

Lösung 5

$$
\begin{aligned}
Z\colon & \mathbb{N}_0 \to \mathcal{P}(\mathbb{N}_0) \\
& n \mapsto \{i \in \mathbb{N}_0 \mid R((\mathrm{Repr}_2(n)))(i) = 1 \text{ und } i < |\mathrm{Repr}_2(n)|\}
\end{aligned}
$$

Erinnerung: Für ein Wort w ist w^R das Spiegelwort von w.

Eine alternative Lösung ist:

$$
n \mapsto \left\{i \in \mathbb{N}_0 \mid (n \ \mathbf{div}\ 2^i) \ \mathbf{mod}\ 2 = 1\right\}
$$

Aufgabe 6 - Quersummen (3 Punkte)

In dieser Aufgabe beschäftigen wir uns mit Teilbarkeitsregeln für Quersummen. Die Quersumme einer Zahl n zur Basis b ist die Summe der Werte aller Ziffern, notiert als

$$Q_b(n) = \sum_{i=0}^{|\mathrm{Repr}_b(n)|-1} \mathrm{Num}_b(\mathrm{Repr}_b(n)(i))$$

Wir wollen die folgende Aussage $\mathcal{A}$ beweisen:
Seien $b, k \in \mathbb{N}_+$, so dass $b > k$ und $b \bmod k = 1$. Dann gilt für jede Zahl n, dass n genau dann durch k teilbar ist, wenn $Q_b(n)$ durch k teilbar ist.

- Nutzen Sie $\mathcal{A}$, um für die folgenden Zahlen zu bestimmen, ob sie durch 3 teilbar sind: 1234; 951753; 852456. (1 Punkt)
- Zeigen Sie $\mathcal{A}$. Sie dürfen dafür annehmen, dass für alle $n, b \in \mathbb{N}_+$ gilt

$$n = \sum_{i=0}^{|\mathrm{Repr}_b(n)|-1} b^i \,\mathrm{Num}_b(R(\mathrm{Repr}_b(n))(i))$$

wobei $R(w)$ das das Spiegelwort von w wie in Blatt 3 Aufgabe 2 ist. (2 Punkte)

Lösung 6

a) Es gilt $Q(1234) = 10, Q(951753) = 30$ und $Q(852456) = 30$, also ist 1234 nicht durch 3 teilbar, aber die anderen beiden sind es.

b) Seien $b, k \in \mathbb{N}_+$ so, dass $b > k$ und $b \bmod k = 1$. Wir zeigen nun, dass $n \bmod k = Q_b(n) \bmod k$, woraus $\mathcal{A}$ folgt.

Für den Fall, dass $k = 1$, ist die Aussage trivial.

Sei nun $k \geq 2$. Dann gilt für $i \in \mathbb{N}_0$:

$$b^i \bmod k = (b \bmod k)^i \bmod k = 1^i \bmod k = 1 \bmod k \overset{k \geq 1}{=} 1$$

Damit folgt:

$$
\begin{aligned}
n \operatorname{\texttt{mod}} k &= \left(\sum_{i=0}^{|\mathrm{Repr}_b(n)|-1} b^i \,\mathrm{Num}_b(R(\mathrm{Repr}_b(n))(i)) \right) \operatorname{\texttt{mod}} k \\
&= \left(\sum_{i=0}^{|\mathrm{Repr}_b(n)|-1} \left(b^i \,\mathrm{Num}_b(R(\mathrm{Repr}_b(n))(i))\right) \operatorname{\texttt{mod}} k \right) \operatorname{\texttt{mod}} k \\
&= \left(\sum_{i=0}^{|\mathrm{Repr}_b(n)|-1} \left(b^i\right) \operatorname{\texttt{mod}} k \cdot (\mathrm{Num}_b(R(\mathrm{Repr}_b(n))(i))) \operatorname{\texttt{mod}} k \right) \operatorname{\texttt{mod}} k \\
&= \left(\sum_{i=0}^{|\mathrm{Repr}_b(n)|-1} 1 \cdot (\mathrm{Num}_b(R(\mathrm{Repr}_b(n))(i))) \operatorname{\texttt{mod}} k \right) \operatorname{\texttt{mod}} k \\
&= \left(\sum_{i=0}^{|\mathrm{Repr}_b(n)|-1} (\mathrm{Num}_b(\mathrm{Repr}_b(n)(i))) \operatorname{\texttt{mod}} k \right) \operatorname{\texttt{mod}} k = 0 \\
&= \left(\sum_{i=0}^{|\mathrm{Repr}_b(n)|-1} \mathrm{Num}_b(\mathrm{Repr}_b(n)(i)) \right) \operatorname{\texttt{mod}} k \\
&= Q_b(n) \operatorname{\texttt{mod}} k
\end{aligned}
$$

Bitte beachten Sie die folgenden Hinweise:

- Lösungen **müssen** handschriftlich erstellt werden
- Ihre Abgabe sollte die erste Seite dieser Datei als Deckblatt haben
- Ihre Abgabe muss **rechtzeitig** erfolgen

Außerdem, wenn Sie Ihre Ausarbeitung über die Abgabekästen im Keller des Informatik-Gebäudes abgeben:

- Ihre Abgabe muss in der oberen **linken** Ecke zusammengeheftet werden
- Tablet-Ausdrucke sind zulässig

Wenn Sie Ihre Ausarbeitung online über ILIAS abgeben, dann achten Sie darauf:

- Ihre Abgabe muss **genau eine** PDF-Datei sein
- Scans und lesbare Fotos sind zulässig
- Abgabe erfolgt unter „Tutorien“ im Ordner **Ihres** Tutoriums