Karlsruher Institut für Technologie

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

Übungsblatt 3

Grundbegriffe der Informatik — Winter 2023/24

Tutor*in: Tutorium Nr.:

Nach-,Vorname 1: ,

Matr.nr. 1:

Nach-,Vorname 2: ,

Matr.nr. 2:

Ausgabe: 14. November 2023, 14:30 Uhr

Abgabe: 24. November 2023, 12:30 Uhr

Bitte beachten Sie die Hinweise auf der letzten Seite.

---

*Von Tutor*in auszufüllen:*

Blatt 3:	/ 19.5	Blätter 1 – 3, Stud. 1:	/ 60
		Blätter 1 – 3, Stud. 2:	/ 60

Aufgabe 1 - Eingeschränkte Funktionen (3 Punkte)

Gegeben seien Mengen A, B, C, D, so dass $A \cap C = B \cap D = \emptyset$.

a) Seien $f : A \to B,\ g : C \to D$ zwei Funktionen. Ist $f \cup g \subseteq (A \cup C) \times (B \cup D)$ auch eine Funktion? Beweisen oder widerlegen Sie. (2 Punkte)

b) Sei nun $h : (A \cup C) \to (B \cup D)$ eine Funktion. Geben Sie Funktionen $h|_A : A \to (B \cup D),\ h|_C : C \to (B \cup D)$ an, so dass $h|_A \cup h|_C = h$. (1 Punkt)

Lösung 1

a) Ja, denn: Sei $h = f \cup g \subseteq (A \cup C) \times (B \cup D)$. Dann gilt:

- h ist linkstotal, denn für jedes $x \in A \cup C$ existiert ein $y \in B \cup D$, sodass $(x, y) \in h$: Falls $x \in A$, existiert per Definition ein $(x, y) \in f$; falls $x \in C$, existiert ein $(x, y) \in g$.
- h ist rechtseindeutig: Nehmen wir zum Widerspruch an, es gäbe $x \in A \cup C,\ y, z \in B \cup D$, so dass $y \neq z$ und $(x, y), (x, z) \in h$.

  Nehmen wir an, dass $(x, y) \in f$. Da f rechtseindeutig ist, muss $(x, z) \notin f$, also $(x, z) \in g$. Also muss $x \in A$ und $x \in C$. Wir haben aber angenommen, dass $A \cap C = \emptyset$.

  Nehmen wir an, dass $(x, y) \in g$, gelangen wir auf analogem Wege auch zu einem Widerspruch.

  Also muss h rechtseindeutig sein.

b) $h|_A = (A \times (B \cup D)) \cap h$, $h|_C = (C \times (B \cup D)) \cap h$

Aufgabe 2 - Fragwürdige Verschlüsselung (3.5 Punkte)

Die Jagd nach Dr. Meta ist nun in vollem Gange. Die GBI hat die Fährte des Superbösewichts aufgenommen und ist entschlossen, ihn dieses Mal dingfest zu-machen. Zum Glück hat sich das Aktensortieren gelohnt! Über die letzten Monate hat die GBI mehrere verdächtige Vorkommnisse verzeichnet, darunter auch auffällig viele Konversationen eines gewissen „R. D. Atem“ mit mehreren Agenten der GBI. Gibt es etwa Spione innerhalb der Organisation?

Dass Dr. Meta die Erfindung der Decknamen wohl seinem Praktikanten überlassen hat, kommt der GBI natürlich sehr gelegen. Vermutlich wurden auch noch andere wichtige Informationen auf diese Art „verschlüsselt“. Ihre Aufgabe ist es nun, dem Team aus vertrauenswürdigen GBI-Agenten zu helfen, Hinweise zu finden. Decknamen sind dabei Wörter beliebiger Länge über einem Alphabet A.

a) Einige Agenten beschweren sich darüber, wie anstrengend es ist, ständig Namen rückwärts lesen zu müssen, um sie mit ihren Daten abzugleichen. Helfen sie Ihnen, indem Sie unten eine induktive Definition der unären Operation R angeben. R soll dabei ein Wort $w \in A^n$ spiegeln, es soll also gelten, dass $(R(w))(i) = w(n-i-1)$ für alle $i \in \mathbb{Z}_n$ ist.[1] (1.5 Punkte)

$$R\colon A^* \to A^*$$
$$w \mapsto \begin{cases} \_\_\_\_\_ & \mid w = \varepsilon \\ \_\_\_\_\_ \cdot \_\_\_\_\_ & \mid \_\_\_\_\_ \end{cases}$$

b) Zeigen oder widerlegen Sie, dass R *selbstinvers* ist, also dass $R(R(w)) = w$ für jedes Wort $w \in A^*$ gilt. (2 Punkte)

Hinweis: Sie können dazu entweder ihre Definition aus Teilaufgabe a) oder die Beschreibung aus der Aufgabenstellung von a) verwenden.

Lösung 2

a)

$$R\colon A^* \to A^*$$
$$w \mapsto \begin{cases} \varepsilon & \mid w = \varepsilon \\ R(w') \cdot w(0), & \mid w = w(0) \cdot w' \end{cases}$$

b) Sei $w \in A^*$ beliebig und sei $i \in \mathbb{Z}_{|w|}$. Dann gilt:

$$\begin{aligned} R(R(w))(i) &= R(w)(|w| - i - 1) \\ &= w(|w| - (|w| - i - 1) - 1) \\ &= w(|w| - |w| + i + 1 - 1) \\ &= w(i) \end{aligned}$$

Damit folgt direkt, das R selbstinvers ist.

Aufgabe 3 - Reißverschlussprinzip (9 Punkte)

Alarmiert davon, wie schnell selbst der geniale Dr. Meta sich durch so eine Fahrlässigkeit angreifbar macht, beschließt die GBI, die Verschlüsselung ihrer eigenen Daten zu verbessern. Die Idee ist, sensible Informationen bis zur Unkenntlichkeit

[1] Wir nennen $R(w)$ auch das Spiegelwort von w und schreiben statt $R(w)$ auch w^R.

miteinander zu vermischen. Da Sie sich im Fall Dr. Meta schon als sehr hilfreich bewiesen haben, fällt Ihnen diese Aufgabe zu.

Sei im Folgenden ein Alphabet A gegeben. Gegeben seien zwei Wörter $w_1 \in A^n, w_2 \in A^m$ über A. Die Verschränkung $w_1 \between w_2$ von w_1 und w_2 ist ein Wort $w \in A^{n+m}$, das abwechselnd die Zeichen von w_1 und w_2 enthält. Dabei ist das erste Zeichen von w das erste Zeichen von w_1. Ist $n \neq m$, so werden die übrigen nicht verschränkten Zeichen des längeren Wortes unverändert an das Ende von w übernommen.

So ist zum Beispiel $\texttt{meta} \between \texttt{informatik} = \texttt{mientfaormatik}$.

a) Geben Sie $\texttt{streng} \between \texttt{geheim}$ an. (0.5 Punkte)

b) Wir betrachten zunächst nur den Fall, dass $n = m$ gilt. Geben Sie dafür eine Definition für die Funktion $\between^{=}\colon \bigcup_{n\in\mathbb{N}}(A^n \times A^n) \to A^*$ an, die zwei Worten gleicher (aber beliebiger) Länge ihre Verschränkung zuweist. Es soll also für alle $n \in \mathbb{N}$ und für alle $w_1, w_2 \in A^n$ gelten, dass $w_1 \between^{=} w_2 = w_1 \between w_2$. (2 Punkte)

Bei der Arbeit mit Wörtern ist es hilfreich, wenn man „Anfangsteile“ oder „Endteile“ von Wörtern verwenden kann. Für eine Aufteilung eines Wortes $w = w_{pre} \cdot w_{post}$ nennen wir w_{pre} ein *Präfix* von w und w_{post} ein *Postfix* von w. Für eine natürliche Zahl $n \leq |w|$ bezeichne $\texttt{pre}(w, n)$ das Präfix der Länge n von w und $\texttt{post}(w, n)$ das Postfix der Länge n von w.

c) Als GBI-Agent:in können Sie Ihre Expertise aus der letzten Aufgabe ins Spiel bringen: Die Funktion `post` lässt sich mit Hilfe der Funktionen R aus Aufgabe 2 und `pre` definieren. Geben Sie dazu für ein Wort $w \in A^*$ und eine natürliche Zahl $n \leq |w|$ einen Ausdruck an, der $\texttt{post}(w, n)$ berechnet und nur die Funktionen `pre` und R verwendet (und natürlich w und n). (1 Punkt)

d) Geben Sie eine Definition für $\between$ an. (2 Punkte)

Hinweis: Greifen Sie bei Ihrer Definition auf die Funktionen $\between^{=}$, `pre` und `post` zurück und machen Sie eine Fallunterscheidung.

e) Zeigen Sie für beliebige Wörter $w_1, w_2 \in A^*$ mit $|w_1| = |w_2|$: Es gilt $w_1 \between w_2 = w_2 \between w_1$ genau dann, wenn $w_1 = w_2$. (2.5 Punkte)

f) Seien nun $w_1, w_2, w_3 \in A^*$ mit $|w_3| = l$. Beweisen oder widerlegen Sie: Wenn w_1 und w_2 Präfixe von w_3 sind, dann gilt $(w_1 \between w_2) \between w_3 = w_1 \between (w_2 \between w_3)$. (1 Punkt)

Lösung 3

a) $\texttt{streng} \between \texttt{geheim} = \texttt{sgterheenigm}$

b) Seien $w_1, w_2 \in A^n$. Dann ist

$$w_1 \between^= w_2 \colon \mathbb{Z}_{2n} \to A$$
$$i \mapsto \begin{cases} w_1(\frac{i}{2}) & \mid i \text{ ist gerade} \\ w_2(\frac{i-1}{2}) & \mid i \text{ ist ungerade} \end{cases}$$

c) Sei $w \in A^*$ und sei $n \in \mathbb{Z}_{|w|}$. Dann ist

$$\texttt{post}(w, n) = R(\texttt{pre}(R(w), n))$$

d)

$$\between \colon A^* \times A^* \to A^*$$
$$(w_1, w_2) \mapsto \begin{cases} (\texttt{pre}(w_1, |w_2|) \between^= w_2) \cdot \texttt{post}(w_1, |w_1| - |w_2|) & \mid |w_1| \geq |w_2| \\ (w_1 \between^= \texttt{pre}(w_2, |w_1|)) \cdot \texttt{post}(w_2, |w_2| - |w_1|) & \mid |w_1| < |w_2| \end{cases}$$

e) Seien $w_1 \in A^n$ und $w_2 \in A^n$ zwei beliebige Wörter der gleichen Länge. Dann ist $\texttt{post}(w_1, n-n) = \texttt{post}(w_2, n-n) = \varepsilon$, also ist $w_1 \between w_2 = w_1 \between^= w_2$ und $w_2 \between w_1 = w_2 \between^= w_1$. Also:

„⇒“ Es gelte $w_1 \between w_2 = w_2 \between w_1$. Dann muss für $w = w_1 \between w_2$ gelten, dass $w(i) = w(i+1)$ für gerade $i < n-1$, denn es ist

$$\begin{aligned} w(i) &= (w_1 \between^= w_2)(i) \\ &= w_1\left(\frac{i}{2}\right) && \text{weil } i \text{ gerade} \\ &= w_1\left(\frac{i+1-1}{2}\right) \\ &= (w_2 \between^= w_1)(i+1) && \text{weil } i+1 \text{ ungerade} \\ &= w(i+1) \end{aligned}$$

Da außerdem

$$w(i+1) = (w_1 \between^= w_2)(i+1) = w_2\left(\frac{(i+1)-1}{2}\right) = w_2\left(\frac{i}{2}\right)$$

folgt direkt, dass für $j \in \mathbb{Z}_n$ gilt, dass $w_1(j) = w_2(j)$.

„⇐“ Sei $w_1 = w_2$. Dann ist

$$\begin{aligned} w_1 \between w_2 &= (w_1 \between^{=} \texttt{pre}(w_1, n)) \cdot \texttt{post}(w_2, n-n) \\ &= (w_1 \between^{=} w_2) \cdot \varepsilon \\ &= (w_2 \between^{=} w_1) \cdot \varepsilon \\ &= (w_2 \between^{=} \texttt{pre}(w_1, n)) \cdot \texttt{post}(w_2, n-n) \\ &= w_2 \between w_1 \end{aligned}$$

f) Wir widerlegen die Behauptung durch ein Gegenbeispiel. Sei dazu $A = \{\texttt{a}, \texttt{b}\}$ und seien $w_1 = \texttt{ab}, w_2 = \texttt{ab}, w_3 = \texttt{abba}$. Dann ist $w_1 = \texttt{pre}(w_3, 2)$ und $w_2 = \texttt{pre}(w_3, 2)$, aber

$$\begin{aligned} (w_1 \between w_2) \between w_3 &= (\texttt{ab} \between \texttt{ab}) \between \texttt{abba} \\ &= \texttt{aabb} \between \texttt{abba} \\ &= \texttt{aaabbbba} \\ &\neq \texttt{aababbba} \\ &= \texttt{ab} \between \texttt{aabbba} \\ &= \texttt{ab} \between (\texttt{ab} \between \texttt{abba}) \\ &= w_1 \between (w_2 \between w_3) \end{aligned}$$

Aufgabe 4 - Alea iacta est. (4 Punkte)

Gegeben seien ein Alphabet A und die folgende Funktion `dice`, die das Bild eines Wortes über A „durcheinanderwürfelt“:

$$\begin{aligned} \texttt{dice}\colon \bigcup_{n \in \mathbb{N}_+} (A^n \times \mathbb{Z}_n^n) &\to A^* \\ \texttt{dice}(w, v)(i) &= w(v(i)) \end{aligned}$$

Dabei ist $v(i)$ die i-te Komponente des Tupels v.

a) Seien $w = \texttt{confuse}$ und $v = (3, 1, 0, 4, 5, 6, 5)$. Geben Sie $\texttt{dice}(w, v)$ an. (0.5 Punkte)

b) Geben Sie alle $v \in \mathbb{Z}_2^2$ an, für die es ein $u \in \mathbb{Z}_2^2$ so gibt, dass für alle Wörter $w \in A^2$ gilt: $\texttt{dice}(\texttt{dice}(w, v), u) = w$. Begründen Sie, warum Ihre Antwort korrekt ist. (2 Punkte)

c) Sei $n \in \mathbb{N}$ beliebig. Geben Sie die Menge aller $v \in \mathbb{Z}_n^n$ an, für die es ein $u \in \mathbb{Z}_n^n$ gibt, so dass für alle Wörter $w \in A^n$ gilt: $\texttt{dice}(\texttt{dice}(w, v), u) = w$.

(1.5 Punkte)

Lösung 4

a) $\texttt{dice}(w, v) = \texttt{focuses}$

b) Es gibt zwei Tupel in $\mathbb{Z}_2^2 = \{(0,0), (0,1), (1,0), (1,1)\}$, die die Anforderung erfüllen, und zwar $(0,1)$ und $(1,0)$. Sei $w = w_0 \cdot w_1 \in A^2$. Dann gilt:

$$\begin{aligned}
\texttt{dice}(\texttt{dice}(w, (0,1)), (0,1)) &= \texttt{dice}(\texttt{dice}(w_0 \cdot w_1, (0,1)), (0,1)) \\
&= \texttt{dice}(w_0 \cdot w_1, (0,1)) \\
&= w_0 \cdot w_1 \\
&= w
\end{aligned}$$

$$\begin{aligned}
\texttt{dice}(\texttt{dice}(w, (1,0)), (1,0)) &= \texttt{dice}(\texttt{dice}(w_0 \cdot w_1, (0,1)), (0,1)) \\
&= \texttt{dice}(w_1 \cdot w_0, (0,1)) \\
&= w_0 \cdot w_1 \\
&= w
\end{aligned}$$

Die Tupel $(0,0)$ und $(1,1)$ erfüllen unsere Anforderungen nicht. Dies zeigen wir anhand des Beispiels $w = \texttt{ab}$: Es gilt $\texttt{dice}(w, (0,0)) = \texttt{aa}$. Es kann kein Tupel u geben, sodass $\texttt{dice}(\texttt{aa}, u)$ auf das Zeichen $\texttt{b}$ abbildet. Genauso kann es kein Tupel u' geben, sodass $\texttt{dice}(\texttt{dice}(\texttt{ab}, (1,1)), u') = \texttt{dice}(\texttt{bb}, u')$ auf das Zeichen $\texttt{a}$ abbildet.

c)

$$\begin{aligned}
&\{v \in \mathbb{Z}_n^n \mid \text{ Für alle } i \in \mathbb{Z}_n \text{ gibt es } j \in \mathbb{Z}_n \text{ so, dass } v(j) = i\} \\
&= \{f : \mathbb{Z}_n \to \mathbb{Z}_n \mid f \text{ ist bijektiv}\} \\
&= S_n \qquad \text{(die Menge aller Permutationen über } n \text{ Elementen)}
\end{aligned}$$

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