

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 $f : A \rightarrow B$, $g : C \rightarrow D$ 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 $h : (A \cup C) \rightarrow (B \cup D)$ eine Funktion. Geben Sie Funktionen $h|_A : A \rightarrow (B \cup D)$, $h|_C : C \rightarrow (B \cup D)$ an, so dass $h|_A \cup h|_C = h$. (1 Punkt)

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 beschwerten 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)

$$R: A^* \rightarrow A^*$$

$$w \mapsto \left\{ \begin{array}{l} \underline{\hspace{4cm}} \\ \underline{\hspace{4cm}} \cdot \underline{\hspace{2cm}} \end{array} \right. \quad \left| \begin{array}{l} w = \varepsilon \\ \underline{\hspace{4cm}} \end{array} \right.$$

- 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.

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

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 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 $w_1 \bowtie w_2$ 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 `meta` \bowtie `informatik` = `mientfaormatik`.

- a) Geben Sie `streng` \bowtie `geheim` an. (0.5 Punkte)
- b) Wir betrachten zunächst nur den Fall, dass $n = m$ gilt. Geben Sie dafür eine Definition für die Funktion $\bowtie^= : \bigcup_{n \in \mathbb{N}} (A^n \times A^n) \rightarrow A^*$ 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 $w_1 \bowtie^= w_2 = w_1 \bowtie w_2$. (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 $\text{pre}(w, n)$ das Präfix der Länge n von w und $\text{post}(w, n)$ 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 $\text{post}(w, n)$ berechnet und nur die Funktionen `pre` und R verwendet (und natürlich w und n). (1 Punkt)
- d) Geben Sie eine Definition für \bowtie an. (2 Punkte)
Hinweis: Greifen Sie bei Ihrer Definition auf die Funktionen $\bowtie^=$, `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 $w_1 \bowtie w_2 = w_2 \bowtie w_1$ 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 $(w_1 \bowtie w_2) \bowtie w_3 = w_1 \bowtie (w_2 \bowtie w_3)$. (1 Punkt)

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“:

$$\text{dice}: \bigcup_{n \in \mathbb{N}_+} (A^n \times \mathbb{Z}_n^n) \rightarrow A^*$$
$$\text{dice}(w, v)(i) = w(v(i))$$

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

- Seien $w = \text{confuse}$ und $v = (3, 1, 0, 4, 5, 6, 5)$. Geben Sie $\text{dice}(w, v)$ an. (0.5 Punkte)
- 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: $\text{dice}(\text{dice}(w, v), u) = w$. Begründen Sie, warum Ihre Antwort korrekt ist. (2 Punkte)
- 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: $\text{dice}(\text{dice}(w, v), u) = w$. (1.5 Punkte)

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