Grundbegriffe der Informatik — Aufgabenblatt 6

Tutorium Nr.:		Tutor*in:	
Matr.nr. 1:			
Nach-,Vorname 1:		,	
Matr.nr. 2:			
Nach-,Vorname 2:		,	

Ausgabe:	26. Nobember 2021, 12:00 Uhr
Abgabe:	03. Dezember 2021, 12:30 Uhr in dem Holzkasten neben Raum -119 im UG des Info-Gebäudes (50.34)

Lösungen werden nur korrigiert, wenn sie

- handschriftlich erstellt sind (Tablet-Ausdruck erlaubt) und
- mit dieser Seite als Deckblatt
- in der oberen **linken** Ecke zusammengeheftet

rechtzeitig abgegeben werden.

Abgaberegeln für Teilnehmer der Online-Tutorien:

- handschriftlich erstellt (lesbare Fotos akzeptiert)
- **rechtzeitig**, mit diesem Deckblatt in **genau einer** PDF-Datei
- direkt an den entsprechenden Tutor abgeben.

---

*Von Tutor*in auszufüllen:* erreichte Punkte

Blatt 6:	/ 17	Blätter 1 – 6, Stud. 1:	/ 116,5
		Blätter 1 – 6, Stud. 2:	/ 116,5

Aufgabe 6.1 (0,5 + 2 + 1 + 2 + 1 + 1 + 1,5 = 9 Punkte)
Sei A das Alphabet der Zeichen $\{\text{␣}, \texttt{a}, \texttt{b}, ..., \texttt{z}, .\}$. Eine vollständige Auflistung der Zeichen aus A finden Sie in der unten aufgeführten Tabelle in Zeilen eins und drei. Sei außerdem eine Abbildung $val : A \to \mathbb{Z}_{28}$ definiert, deren Wert in Zeile zwei, bzw. vier der unteren Tabelle für jedes $x \in A$ explizit aufgelistet ist. Ferner sei die Umkehrfunktion von val als $val^{-1} : \mathbb{Z}_{28} \to A$ definiert. val^{-1} bildet jede Zahl $n \in \mathbb{Z}_{28}$ auf das entsprechende $x \in A$, mit $val(x) = n$ ab.

$x \in A$	␣	a	b	c	d	e	f	g	h	i	j	k	l	m
$val(x)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$x \in A$	n	o	p	q	r	s	t	u	v	w	x	y	z	.
$val(x)$	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Damit die Daten der B.I.R.Ds auf dem Weg zu seiner geheimen Zentrale vertraulich bleiben, hat sich Dr. Meta eine Verschlüsselungsfunktion $Enc : A^* \times A^+ \to A^*$ überlegt. Seit seiner Promotion ist er allerdings des Definierens von Funktionen überdrüssig. Da Sie ihre Fähigkeiten auf diesem Gebiet bereits zum wiederholten Male unter Beweis gestellt haben, dürfen Sie diese Aufgabe für ihn übernehmen. Die Verschlüsselung soll eine Nachricht $w \in A^*$, sowie einen Schlüssel $k \in A^+$ wie folgt verarbeiten:
Zum Verschlüsseln eines Zeichens der Nachricht wird es mit einem Zeichen des Schlüsselwortes „aufaddiert". Hierzu wird zunächst mittels val der Zahlenwert der jeweiligen Zeichen berechnet. Diese Werte werden addiert und das Ergebnis wird mittels val^{-1} wieder auf ein Zeichen aus A abgebildet. Die verschlüsselte Nachricht ergibt sich als Konkatenation aller jeweils auf diese Weise verschlüsselten Zeichen. Hierbei wird für alle $i \in \mathbb{Z}_{|w|}$ $w(i)$ unter Verwendung von $k(i)$ verschlüsselt.
Die folgenden Teilaufgaben führen Sie schrittweise zur Definition von Enc:

a) Damit die oben beschriebene Rückberechnung eines Zeichens mit val^{-1} für alle Ergebnisse s einer Addition zweier Zeichenwerte stets funktioniert, muss sichergestellt werden, dass stets $s \in \mathbb{Z}_{28}$ gilt. Welche in der Vorlesung vorgestellte Operation kann verwendet werden um dies sicherzustellen?

b) Definieren Sie eine Funktion $first_n : A^m \to A^n$, die für beliebige $m, n \in \mathbb{N}_0$, mit $m \geq n$ und alle Wörter $w \in A^m$ das Präfix der Länge n von w berechnet.
Tipp: Nutzen Sie eine Hilfsfunktion.
Tipp: Setzen Sie Funktionsargumente ähnlich wie in Aufgabe 5.4 illustriert ein.

c) Damit die gesamte Nachricht w zeichenweise verschlüsselt werden kann, muss für den Schlüssel k stets $|w| \leq |k|$ gelten. Damit sich Dr. Meta keine langen Schlüsselwörter merken muss, soll für den Fall $|k| < |w|$ die Zeichen des Schlüsselwortes Reihenfolge getreu „recycelt" werden. Definieren Sie die Funktion $pad_n : A^+ \to A^n$, die für ein konkretes $n \in \mathbb{N}_0$ und Eingaben $w \in A^+$ im Fall $|w| \geq n$ das Präfix der Länge n und im Fall $|w| < n$ eine Reihenfolge getreue Wiederholung der Zeichen in w mit insgesamt Länge n ausgibt.
Bsp: $pad_{12}(\texttt{dr␣meta}) = \texttt{dr␣metadr␣me}$ $pad_4(\texttt{metamorphose}) = \texttt{meta}$

d) Definieren Sie die Funktion Enc.

e) Wie viele Rechtsinverse hat Enc? Beweisen Sie.

f) Ist Enc eine Codierung im Sinne der Vorlesung oder nicht? Beweisen Sie.

g) Die Folgende Nachricht wurde von den B.I.R.D-Drohnen gesendet:
„`wnlgbnovtezjznqquqtaoneejfmifxfb␣nez.j␣iem.`"
Sie ist mit Dr. Metas Universalpasswort „`genial␣boese`" verschlüsselt. Entschlüsseln Sie sie und geben sie die originale Nachricht an. Rechenweg **nicht** gefordert.

Aufgabe 6.2 (2 [+ 3] = 2 [+ 3] Punkte)

a) Bilden Sie den Huffman-Baum zum Wort $w =$ `fachschaftsschach`.
Beginnen Sie mit folgender Zeichenanordnung der Blätter:
`f t h s a c`
Bilden Sie einen Baum ohne kreuzende Kanten.
Geben Sie außerdem die Huffman-Codierung jedes Zeichens an.

b) Wie kann die Huffman-Codierung angepasst werden um möglichst kurze Codewörter eines ternären Alphabets $\{0, 1, 2\}$ zu erzeugen?
Orientieren Sie sich an der Beschreibung zur Konstruktion des Huffman-Codes in Kapitel 8 (Folien 62-64). Beschreiben Sie ihre Anpassung möglichst präzise.
Diese Aufgabe gibt 3 Bonuspunkte.

Aufgabe 6.3 (0,5 + 0,5 + 0,5 + 0,5 + 4 = 6 Punkte)

Sei A ein beliebiges Alphabet mit $|A| > 2$. Definieren Sie die in den folgenden Teilaufgaben die in natürlicher Sprache spezifizierten Dinge **formal korrekt**. Nutzen sie hierfür keine natürliche Sprache, mit Ausnahme folgender Begriffe:
„für alle“ „es gibt (ein)“, bzw. „gibt es (ein)“

a) Für ein Wort $w \in A^*$ definieren wir das von w induzierte Teilalphabet A_w als die Menge aller Zeichen die sowohl in A als auch in w enthalten sind. Definieren Sie A_w.

b) Eine Verallgemeinerung der Zeichenhäufigkeitsfunktion $N_x(w)$ auf ganze Mengen M, sodass $N_M(w)$ die gesamte Häufigkeit aller Zeichen M in w ergibt. Definieren Sie $N_M(w)$.

c) Für zwei beliebige Mengen von Zeichen, die in w enthalten sind, gilt, dass die Elemente der größeren Menge insgesamt häufiger in w vorkommen. Definieren Sie diesen Zusammenhang für entsprechende Mengen aus A_w.

d) Sei A ein beliebiges Alphabet, $w \in A^*$ ein Wort und $H(w)$ eine Huffman-Codierung von w. Geben Sie eine geschlossene Formel zur Berechnung von $|H(w)|$ ohne Verwendung von $w(i)$ - oder einer äquivalenten Funktion an.

Sei im Folgenden $w \in A^*$ ein Wort, dass die in Aufgabenteil c) spezifizierte Bedingung erfüllt und H eine Huffman-Codierung von w.

e) Gilt für alle $x_1, x_2 \in A_w$: $|H(x_1)| = |H(x_2)|$?
   - Falls ja: Beweisen Sie.
   - Falls nein: Fügen Sie weitere Bedingungen zu w hinzu, sodass die Behauptung gilt. Formulieren Sie die Bedingungen ebenfalls nach den Kriterien aus a) - c). Beweisen Sie, dass die Behauptung aus der Gesamtmenge aller Bedingungen folgt.

   Hinweis: Überlegen Sie sich, wie ein Huffman-Baum aussehen muss, damit die Behauptung erfüllt ist.