Einführung in die Theoretische Informatik

Überblick:

Einführung von formalen Berechnungsmodellen

⇝ Klassifizierung von Problemen } bzgl. ihrer Schwierigkeit

formale Beschreibung was Computer / Algorithmen können

Theoretisch idealisiertes Modell ⇝ Praxis: endlichen Speicher
↳ aber „immer" möglich mehr Speicher zu organisieren

Theorie: Unendlichen Speicher

Wichtiges Konzept: Einschränkungen bzgl. Zeit und Speicher

Probleme: Eingaben (z.B. 0,1-Folgen)

Ausgaben (z.B. 0,1-Folgen) $\rightsquigarrow$ Spezialfall: 0 „Ablehnen"/„Nein"
1 „Annehmen"/„Ja"

1 Grundlagen

1.1 Notation und Begriffe

- $\mathbb{N}$ bezeichnet die $\{1, 2, 3, \dots\}$
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
- Für $n \in \mathbb{N}_0$, sei $[n] = \{1, \dots, n\}$ und $[n]_0 = \{0, 1, \dots, n\}$.
- Für eine Menge A und $n \in \mathbb{N}$ ist $A^n = \{(a_1, \dots, a_n) : a_1, \dots, a_n \in A\}$.

- Für $n \in \mathbb{N}$ ist eine <u>n-äre partielle Funktion</u> $\varphi : A^n \rightsquigarrow B$ eine Funktion mit $\mathrm{dom}(\varphi) \subseteq A^n$ und $\mathrm{Im}(\varphi) \subseteq B$. Für $a_1, \ldots, a_n \in A$ bedeutet $\varphi(a_1, \ldots, a_n)\downarrow$, dass $(a_1, \ldots, a_n) \in \mathrm{dom}(\varphi)$ gilt und $\varphi(a_1, \ldots, a_n)\uparrow$ bedeutet dass $(a_1, \ldots, a_n) \notin \mathrm{dom}(\varphi)$.
  Statt $\varphi(a_1, \ldots, a_n)\uparrow$ schreiben wir auch $\varphi(a_1, \ldots, a_n) = \uparrow$.
  Die part. Funktion φ ist <u>total</u>, wenn $\mathrm{dom}(\varphi) = A^n$ gilt.

- Eine <u>lineare Ordnung</u>, auch <u>totale Ordnung</u>, auf einer Menge A ist eine Relation $\leq \subseteq A^2$, so dass die folgenden Eigenschaften erfüllt sind (wie für Relationen üblich verwenden wir hier Infixnotation, schreiben also für $a, b \in A$ den Ausdruck $a \leq b$ anstatt $(a, b) \in \leq$):

  (i) $a \leq a$ $\quad \forall a \in A$ (<u>Reflexivität</u>)
  „für alle“

  (ii) $a \leq b \wedge b \leq a \Rightarrow a = b$ $\quad \forall a, b \in A$ (<u>Antisymmetrie</u>)
  „und“

  (iii) $a \leq b,\ b \leq c \Rightarrow a \leq c$ $\quad \forall a, b, c \in A$ (<u>Transitivität</u>)

(iv) $a \leq b \lor b \leq a \quad \forall a, b \in A$ (Totalität).

↑ „oder"

1.2 Alphabete, Wörter und Sprachen

Eingaben und Ausgaben in unseren Berechnungsmodellen werden Wörter genannt, wobei wir beliebige Zeichenketten als Wörter zulassen.

Definition 1.1 (Alphabet)

Ein Alphabet ist eine nichtleere endliche Menge Σ. Das Alphabet Σ wird $|\Sigma|$-är bezeichnet. Die Elemente von Σ heißen Buchstaben oder Symbole.

Definition 1.2 (Wörter)

Ein Wort über einem Alphabet Σ ist eine endliche Folge von Symbolen aus Σ. Die Länge eines Wortes w ist $|w|$. Für $i \in [|w|]$ bezeichnet $w(i)$ das i-te Element von w und für Symbole $a_1, \dots, a_n \in \Sigma$ bezeichnet $a_1 a_2 \dots a_n$ das Wort w der Länge n mit $w(i) = a_i \quad \forall i \in [n]$.

Das Wort der Länge 0 heißt leeres Wort und wird mit λ bezeichnet.

Ein Wort w der Länge 1 wird mit dem Symbol $w(1)$ identifiziert.

Definition 1.3 (Binäralphabet, Binärwörter)

Das Alphabet $\{0,1\}$ heißt Binäralphabet. Die Wörter über dem Binäralphabet heißen Binärwörter.

Definition 1.4 (Sprache)

Eine Sprache ist eine Menge von Wörtern über einem gemeinsamen Alphabet Σ.

Einige einfachen grundlegenden Sprachen sind die folgenden.

Definition 1.5

Die Menge aller Wörter über Σ wird mit Σ^* bezeichnet.

Kleene-Stern (Stephen Cole Kleene, 1909-1994)

Für $n \in \mathbb{N}_0$ setzen wir

$$\Sigma^{\leq n} := \{w \in \Sigma^* : |w| \leq n\}$$

$$\Sigma^{=n} := \{ w \in \Sigma^* : |w| = n \}$$

$$\Sigma^{\geq n} := \{ w \in \Sigma^* : |w| \geq n \}$$

$$\Sigma^+ := \Sigma^{\geq 1}.$$

Definition 1.6 (Verkettung)

Für Wörter w_1, w_2 ist die Verkettung $w_1 \circ w_2$, auch $w_1 w_2$, von w_1 und w_2 ist definiert durch

$$w_1 \circ w_2 := w_1(1) \_\_\_ w_1(|w_1|)\, w_2(1) \_\_\_ w_2(|w_2|).$$

Für ein Wort w und $n \in \mathbb{N}_0$ ist w^n induktiv definiert durch $w^n := \lambda$ falls $n=0$ und $w^n := w^{n-1} w$ falls $n \geq 1$.

Für Sprachen L_1, L_2 sei durch $L_1 \circ L_2$, auch $L_1 L_2$, definiert durch

$$L_1 \circ L_2 := \{ w_1 w_2 : w_1 \in L_1, w_2 \in L_2 \}.$$

Für eine Sprache L und $n \in \mathbb{N}_0$ ist L^n induktiv definiert durch $L^n = \{\lambda\}$ falls $n=0$ und $L^n := L \circ L^{n-1}$ falls $n \geq 1$. Zudem sei $L^* := \bigcup_{n \in \mathbb{N}_0} L^n$. Für ein Wort w

und eine Sprache L sei $wL := \{w\} \circ L$ und $Lw := L \circ \{w\}$.

Wir folgen der Konvention, dass $\cdot^n$ und $\cdot^*$ stärker bindet als $\circ$; für Wörter u,v gilt also $uv^n = u \circ (v^n)$. Insbesondere gilt auch $ab^n = a(b^n)$ für Symbole a,b eines Alphabets Σ.

Definition 1.7 (Präfix, Infix, Suffix)

Seien u,v Worte.

(i) u ist Präfix von v, kurz $u \sqsubseteq v$, falls es ein Wort w gibt sodass $uw = v$.

(ii) u ist Infix von v, falls es Wörter w_1, w_2 gibt sodass $v = w_1 u w_2$.

(iii) u ist Suffix von v, falls es ein Wort w gibt, sodass $v = wu$.

Definition 1.8 (präfixfrei)

Eine Sprache heißt präfixfrei, wenn $u \sqsubseteq v \Rightarrow u = v$ $\forall u,v \in L$.

Definition 1.9 (Homomorphismus)

Für Sprachen L und M heißt eine Funktion $\varphi: L \to M$ **Homomorphismus von Sprachen**, wenn $\varphi(uv) = \varphi(u)\varphi(v)$ $\forall u,v \in L$ gilt.

Definition 1.10 (längenlexikographische Ordnung)

Ist Σ ein Alphabet und $\leq$ eine lineare Ordnung auf Σ, so ist die zu $\leq$ gehörige **längenlexikographische Ordnung** $\leq_{llex}$ auf Σ^* die lineare Ordnung für die $u \leq_{llex} v$ genau dann für zwei versch. $u,v \in \Sigma^*$ gilt, wenn eine der folg. Bedingungen gilt:

- $|u| < |v|$
- $|u| = |v|$ und ist $i \in [|u|]$ minimal mit $u(i) \neq v(i)$, so gilt $u(i) \leq v(i)$.

Bemerkung: Oft gehen wir von einer impl. Ordung auf Σ aus.
Ist $\Sigma = \{a_1, \ldots, a_n\}$ so gilt $a_1 \leq \ldots \leq a_n$.

Bemerkung 1.11

Sei Σ ein Alphabet. $\forall w \in \Sigma^*$ ist $\{v \in \Sigma^* : v \leq_{llex} w\}$ endlich.

Dies erlaubt es uns für ein Alphabet Σ die Wörter über Σ in Längenlex. Reihenfolge $w_1, w_2, \ldots$ zu betrachten, wobei wir w_i für $i \in \mathbb{N}$ als kleinstes Element von $\Sigma^* \setminus \{w_1, \ldots, w_{i-1}\}$ gewählt sei.

Wir identifizieren oft $\mathbb{N}_0$ mit $\{0,1\}^*$ indem wir $i \in \mathbb{N}_0$ mit dem Längenlex. Reihenfolge $(i+1)$-ten Wort $w_{i+1} \in \{0,1\}^*$ identifizieren.

$\mathbb{N}_0$	0	1	2	3	...
$\{0,1\}^*$	λ	0	1	00	

Definition 1.12

Es bezeichnet $\text{bin}: \mathbb{N}_0 \to \{0,1\}^*$ die Funktion, für die $\text{bin}(i)$ das in längenlex. Reihenfolge $(i+1)$-te Binärwort ist $\forall i \in \mathbb{N}_0$.

Bemerkung 1.13

$\forall i \in \mathbb{N}_0$ ist $1\,\mathrm{bin}(i)$ die Binärdarstellung von $i+1$. Umgekehrt ist $\forall w \in \{0,1\}^*$ das $\left(2^{|w|} + \sum_{i \in [|w|]} w(i)\, 2^{|w|-i}\right)$-te Binärwort.