Kapitel 1: Grundlagen

Notation:

- sd. : "so dass"
  fa. : "für alle"
  ex : "es existiert"

- leeres Wort: ε
- Σ eine Menge, $u \in \Sigma^* \Rightarrow$ für $i \in \{0, 1, \ldots, |u|-1\}$ schreibe u_i, um das Symbol $u_i \in \Sigma$ an Position i in u zu bezeichnen. Dh: $u = u_0 u_1 \cdots u_{|u|-1}$.

- natürliche Zahlen: $\mathbb{N} := \{0, 1, 2, 3, \ldots\}$
  nat. Zahlen ohne 0 : $\mathbb{N}_{\geq 1} := \mathbb{N} \setminus \{0\}$

- A, B Mengen; $f: A \to B$, $\bar{a} = (a_0, \ldots, a_{k-1}) \in A^k \Rightarrow$
  $$f(\bar{a}) := (f(a_0), \ldots, f(a_{k-1})) \in B^k$$
  $R \subseteq A^k \Rightarrow$
  $$f(R) := \{ f(\bar{a}) : \bar{a} \in R \}$$

- Potenzmenge einer Menge M: $\{X : X \subseteq M\}$:
  $\mathcal{P}(M)$ bzw. $\mathrm{Pot}(M)$ bzw. 2^M

- $u \in \Sigma$

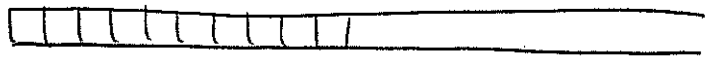
Syntax und Semantik der Logik erster Stufe (FO)

siehe Skript! (Wiederholung: in der 1. Übungsstunde)

Turingmaschinen (TM)

intuitiv:

1 Band, das linksseitig begrenzt ist:



Position 0 1 2 3 4 5 6 ....

Definition (TM)

Eine nichtdeterministische Turingmaschine (NTM)

$$M = (Q, \Sigma, \Gamma, \Delta, q_0, F)$$

besteht aus

- einer endlichen Menge Q von Zuständen
- einem endlichen Arbeitsalphabet Γ mit ausgezeichnetem Blank-Symbol $\Box$
- einem Eingabealphabet $\Sigma \subseteq \Sigma \setminus \{\Box\}$
- einem Anfangszustand $q_0 \in Q$
- einer Menge $F = F_{akz} \dot{\cup} F_{verw} \subseteq Q$ von Endzuständen, die aus einer Menge F_{akz} von akzeptierenden und einer Menge F_{verw} von verwerfenden Zuständen besteht
- einer Übergangsrelation

$$\Delta \subseteq (Q \setminus F) \times \Gamma \times Q \times \Gamma \times \{-1, 0, 1\}$$

M heißt <u>deterministisch</u> (kurz: M ist eine DTM), falls f.a. $q \in Q \setminus F$ und $a \in \Gamma$ genau ein $q' \in Q$, $a' \in \Gamma$ und $m \in \{-1, 0, 1\}$ mit

$$(q, a, q', a', m) \in \Delta$$

existiert. In diesem Fall schreiben wir oft

$$M = (Q, \Sigma, \Gamma, \delta, q_0, F)$$

mit Überführungsfunktion $\delta : (Q \setminus F) \times \Gamma \to Q \times \Gamma \times \{-1, 0, 1\}$

<u>Definition</u> (Konfiguration einer TM)

<u>(a)</u> Eine <u>Konfiguration</u> einer TM $M = (Q, \Sigma, \Gamma, \Delta, q_0, F)$ ist ein Tripel

$$C = (q, p, u) \in Q \times \mathbb{N} \times \Gamma^*$$

mit $p \leq |u|$.

<u>Idee</u>: $C = (q, p, u)$ gibt an, dass die TM sich im Zustand q befindet, der Kopf an Position p steht und die Inschrift des Arbeitsbandes u ist.

<u>(b)</u> $\mathcal{C}_M := Q \times \mathbb{N} \times \Gamma^*$ bezeichnet die Menge aller möglichen Konfigurationen von M.

(c) Die <u>Startkonfiguration</u> von M bei Eingabe $w \in \Sigma^*$ ist

$$C_0(w) := (q_0, 0, w\square)$$

(d) Eine Konfiguration $c = (q, p, u)$ heißt <u>Endkonfiguration</u>, falls $q \in F$.
Sie heißt <u>akzeptierend</u>, falls $q \in F_{akz}$, und verwerfend, falls $q \in F_{verw}$

<u>Definition</u> (Lauf einer TM)

Sei $M = (Q, \Sigma, \Gamma, \Delta, q_0, F)$ eine TM.

(a) Die Übergangsrelation Δ induziert eine (partielle) Funktion

$$Next_M : \mathcal{C}_M \to \mathcal{P}ot(\mathcal{C}_M),$$

wobei für $C = (q, p, u) \in \mathcal{C}_M$ gilt:

$$Next_M(C) := \left\{ (q', p', u') : \begin{array}{l} \text{es gibt } a, b \in \Gamma \text{ und} \\ m \in \{-1, 0, 1\}, \text{ s.d. } (q, a, q', b, m) \in \Delta, \\ p' = p + m, \quad u_p = a, \quad u'_p = b, \\ u'_i = u_i \text{ f.a. } i \neq p \text{ und} \\ \bullet\ |u'| = |u|, \text{ falls } p' < |u|, \text{ bzw} \\ \bullet\ |u'| = |u| + 1 \text{ und } u'_{p'} = \square, \text{ falls } p' = |u| \end{array} \right\}$$

D.h.: $Next_M(C)$ enthält alle Konfigurationen, in die M von C aus in <u>einem</u> Schritt gelangen kann.

<u>Beachte</u>: Ist M deterministisch, so ist

$$|Next_M(C)| \leq 1 \quad \text{f.a. } C \in \mathcal{C}_M .$$

(<u>b</u>) Auf Eingabe $w \in \Sigma^*$ definiert M einen <u>Berechnungsbaum</u> $B_M(w)$ wie folgt:

- Der Baum hat einen mit $C_0(w)$ beschrifteten Wurzelknoten.
- Ist v ein mit C beschrifteter Knoten im Baum, so hat v für jedes $C' \in Next_M(C)$ einen Kindknoten mit Beschriftung C'.

(<u>c</u>) Ein <u>Lauf</u> von M bei Eingabe w ist ein Pfad im Berechnungsbaum, der an der Wurzel beginnt und entweder unendlich lang ist oder in einer Endkonfiguration endet (der Lauf heißt dann <u>endlich</u> bzw. <u>terminierend</u>).

(d) Ein Lauf heißt <u>akzeptierend</u> (bzw. <u>verwerfend</u>), falls er in einer akzeptierenden (bzw. verwerfenden) Endkonfiguration endet.

<u>Definition</u> (Sprache einer TM)

(a) Eine TM M <u>akzeptiert</u> eine Eingabe $w \in \Sigma^*$, falls es (mindestens) einen akzeptierenden Lauf von M auf w gibt.
M <u>verwirft</u> w, falls alle terminierenden Läufe von M auf w verwerfen.

(b) Die <u>Sprache</u>
$$L(M) := \{ w \in \Sigma^* : M \text{ akzeptiert } w \}$$
heißt die von M akzeptierte Sprache

(c) Eine Sprache $L \subseteq \Sigma^*$ heißt <u>semi-entscheidbar</u>, falls es eine TM M mit $L(M) = L$ gibt

(d) Eine Sprache $L \subseteq \Sigma^*$ heißt <u>entscheidbar</u>, falls es eine TM M mit $L(M) = L$ gibt, so dass jeder Lauf von M auf jeder Eingabe $w \in \Sigma^*$ terminiert.

<u>Satz:</u>
Jede durch eine NTM (semi-) entscheidbare Sprache L ist auch durch eine DTM (semi-) entscheidbar.

<u>Beweis:</u> Übung.

<u>Satz</u> (hier ohne Beweis)
Das <u>Halteproblem H_ε auf leerem Eingabewort</u>

<u>Eingabe:</u> Eine DTM M
<u>Frage:</u> Hält M bei Eingabe des leeren Worts ε?
(Dh: Ist $B_M(\varepsilon)$ endlich?)

ist nicht entscheidbar (aber semi-entscheidbar).

Der Satz von Trakhtenbrot

Eine (funktionenfreie, endliche) Signatur ist eine endliche Menge

$\sigma = \{\underbrace{R_1, \dots, R_k}_{\text{Relationssymbole}}, \underbrace{c_1, \dots, c_\ell}_{\text{Konstantensymbole}}\}$ mit $k, \ell \in \mathbb{N}$

Jedes R_i hat eine feste Stelligkeit $ar(R_i) \in \mathbb{N}_{\geq 1}$.

Definition:
Sei σ eine (funktionenfreie, endliche) Signatur.
Das endliche Erfüllbarkeitsproblem für $FO[\sigma]$ ist das Berechnungsproblem mit

Eingabe: Ein $FO[\sigma]$-Satz φ

Frage: Gibt es eine endliche σ-Struktur $\mathfrak{A}$ mit $\mathfrak{A} \models \varphi$?

Theorem (Der Satz von Trakhtenbrot, 1950)
Es gibt eine (endliche, funktionenfreie) Signatur σ, so dass das endliche Erfüllbarkeitsproblem für $FO[\sigma]$ unentscheidbar ist.

Beweis:

siehe Tafel, bzw. Skript, Kapitel 1.3.4

Bemerkung:

Man kann sogar zeigen, dass der Satz von Trakhtenbrot für die Signatur $\sigma := \{E\}$ gilt, die aus einem 2-stelligen Relationssymbol E besteht.

(Details: Übung)