Kapitel 1:
Grundlagen und der Satz von Trakhtenbrot

Notation:

- s.d. : "so dass"
- f.a. : "für alle"
- ex. : "es existiert"/ "es gibt"

- natürliche Zahlen:
  $\mathbb{N} := \{0,1,2,\dots\}$
  $\mathbb{N}_{\geq 1} := \mathbb{N} \setminus \{0\}$

- leeres Wort: ε
- $\Sigma^+ := \Sigma^* \setminus \{\varepsilon\}$
- f.a. $w \in \Sigma^+$, für $n := |w|$ und f.a. $i \in \{0,1,\dots,n-1\}$ schreibe w_i, um das Symbol an Position i in w zu bezeichnen.
  D.h.: $w = w_0 w_1 \cdots w_{n-1}$
- Potenzmenge einer Menge M:
  $\mathcal{P}(M) := \mathrm{Pot}(M) := 2^M := \{X : X \subseteq M\}$
- A, B Mengen, $f : A \to B$, $\bar{a} = (a_1,\dots,a_k) \in A^k$
  $\Rightarrow f(\bar{a}) := (f(a_1),\dots,f(a_k)) \in B^k$
- $R \subseteq A^k \to f(R) := \{f(\bar{a}) : \bar{a} \in R\}$

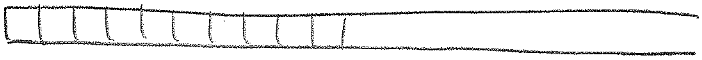
Syntax und Semantik der Logik erster Stufe (FO):

siehe Skript zur Vorlesung "Logik in der Informatik" (N. Schweikardt, HU Berlin).
Wiederholung dazu: in der 1. Übungsstunde

Turingmaschinen (TM)

intuitiv:

1 Band, das linksseitig begrenzt ist:



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

Definition 1.1 (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 $\Sigma \subseteq \Gamma \setminus \{\Box\}$
- 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 <u>Überführungsfunktion</u> $\delta : (Q \setminus F) \times \Gamma \to Q \times \Gamma \times \{-1, 0, 1\}$

<u>Definition</u> 1.2 (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 $p < |u|$.

<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> $\mathcal{C}_M := \{(q, p, u) \in Q \times \mathbb{N} \times \Gamma^* : p < |u|\}$

bezeichnet die Menge aller möglichen Konfigurationen von M.

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

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

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

Definition 1.3 (Lauf einer TM)

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

(a) Die Übergangsrelation Δ induziert eine Funktion

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

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

$Next_M(C) = \{ (q', p', u') :$ es gibt ein Tupel $(q, a, q', b, m) \in \Delta$, so dass gilt:
$p' = p + m$, $u_p = a$, $u'_p = b$,
$u'_i = u_i$ f.a. $i \neq p$ und
- $|u'| = |u|$, falls $p' < |u|$, bzw.
- $|u'| = |u| + 1$ und $u'_{p'} = \Box$, falls $p' = |u|$ $\}$

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>) Ein <u>Lauf</u> von M bei Eingabe w ist ein Tupel $\mathcal{L} = (C_0, C_1, \dots)$ von Konfigurationen von M, so dass gilt:

- $C_0 = C_0(w)$ (Startkonfiguration von M bei Eingabe w)
- $C_i \in Next_M(C_{i-1})$, f.a. $i \geq 1$, und
- entweder ist das Tupel $\mathcal{L}$ unendlich lang, oder es endet mit einer Endkonfiguration. Im letzteren Fall heißt der Lauf dann <u>endlich</u> bzw. <u>terminierend</u>.

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

<u>Definition 1.4</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 <u>alle</u> 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.

Aus der Veranstaltung "Einführung in die Theoretische Informatik" (HU Berlin) sind die beiden folgenden Sätze bekannt (hier ohne Beweise):

<u>Satz 1.5</u>

Jede durch eine NTM entscheidbare (bzw. semi-entscheidbare) Sprache ist auch durch eine DTM entscheidbar (bzw. semi-entscheidbar).

<u>Satz 1.6</u>

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 ?

ist nicht entscheidbar (aber semi-entscheidbar).

Der Satz von Trakhtenbrot

Boris A. Trakhtenbrot: russisch-israelischer Mathematiker, *1921
Alternative Schreibweisen: Trachtenbrot, Trahenbrot
Original-Schreibweise (kyrillisch): Трахтенброт

Definition 1.7

Eine funktionenfreie, endliche Signatur (im Folgenden kurz: Signatur) ist eine endliche Menge

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

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

Definition 1.8

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 $\mathcal{A}$ mit $\mathcal{A} \models \varphi$?

Theorem 1.9 (Der Satz von Trakhtenbrot, 1950)

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

Beweis: Durch Widerspruch:

Angenommen, das endliche Erfüllbarkeitsproblem für $\mathrm{FO}[\sigma]$ ist doch entscheidbar.

Zeige, dass dann auch das Halteproblem H_ε entscheidbar ist.

Ansatz:

Gegeben: Eine DTM M

Frage: Hält M bei Eingabe ε?

Lösung: Repräsentiere die Berechnung von M bei Eingabe ε durch einen $\mathrm{FO}[\sigma]$-Satz φ_M, so dass gilt:

φ_M hat ein endliches Modell $\iff$ der Lauf von M bei Eingabe ε terminiert.

Konstruktion der Formel φ_M:

O.B.d.A. können wir annehmen, dass

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

DTM ist mit

- $Q = \{0, 1, \ldots, s_Q\}$ für ein $s_Q \in \mathbb{N}$
- Anfangszustand $q_0 = 0$
- $F \subseteq Q$
- $\Gamma = \{0, 1, \ldots, s_\Gamma\}$ für ein $s_\Gamma \in \mathbb{N}$
- Blank-Symbol $\square = 0$
- $s := \max\{s_Q, s_\Gamma\}$
- falls der Lauf von M bei Eingabe ε terminiert, so nach genau n Schritten, wobei n eine natürliche Zahl $\geq s$ ist
  (Übung: überlegen, wie "$n \geq s$" o.B.d.A. gewährleistet werden kann)

Die Signatur σ wird (unabhängig von der konkreten DTM M) wie folgt gewählt:

$$\sigma := \{<, \mathit{succ}, 0, B, K, Z\},$$

wobei

- $<$ und succ zwei 2-stellige Relationssymbole,
- 0 ein Konstantensymbol,
- B ein 3-stelliges Relationssymbol und
- K und Z zwei 2-stellige Relationssymbole sind.

Wir geben FO[σ]-Formeln an, die in ihren Modellen $\mathcal{A}$ folgende Interpretationen der Prädikate erzwingen:

(1) $<^{\mathcal{A}}$ ist eine strikte lineare Ordnung, $0^{\mathcal{A}}$ deren kleinstes Element, und $succ^{\mathcal{A}}$ ist die Nachfolger-Relation (engl: successor) bzgl $<^{\mathcal{A}}$, d.h. es gilt

$(a,b) \in succ^{\mathcal{A}} \iff a <^{\mathcal{A}} b$ und es gibt kein c mit $a <^{\mathcal{A}} c <^{\mathcal{A}} b$.

(2) $(t,p,\gamma) \in B^{\mathcal{A}} \iff$

auf Bandposition p steht zum Zeitpunkt t des Laufs von M bei Eingabe ε das Symbol γ

(3) $(t,p) \in K^{\mathcal{A}} \iff$
der Schreib-/Lesekopf von M steht zum Zeitpunkt t des Laufs von M bei Eingabe ε auf Bandposition p

(4) $(t,q) \in Z^{\mathcal{A}} \iff$
M ist zum Zeitpunkt t des Laufs von M bei Eingabe ε in Zustand q.

Wir definieren eine σ-Struktur $\mathcal{A}_M$, die den Lauf von M bei Eingabe ε repräsentiert, wie folgt:

Das Universum von $\mathcal{A}_M$ ist die Menge

$$A_M := \begin{cases} \{0,\dots,n\}, & \text{falls der Lauf von } M \text{ bei Eingabe } \varepsilon \text{ in Schritt } n \in \mathbb{N} \text{ terminiert} \\ \mathbb{N} & \text{falls der Lauf von } M \text{ bei Eingabe } \varepsilon \text{ nicht terminiert} \end{cases}$$

Die Relationen $<^{\mathcal{A}_M}$ und $succ^{\mathcal{A}_M}$ sowie die Konstante $0^{\mathcal{A}_M}$ sind durch die natürliche strikte lineare Ordnung auf A_M, deren Nachfolger-Relation sowie die Zahl 0 belegt.

Die Relationen $B^{\mathcal{A}_M}$, $K^{\mathcal{A}_M}$, $Z^{\mathcal{A}_M}$ sind genau so gewählt, wie in den Punkten (2), (3) und (4) beschrieben.

Wir definieren nun einen FO[σ]-Satz φ_M, der erzwingen soll, dass die Modelle $\mathcal{A}$ von φ_M eine zur Struktur $\mathcal{A}_M$ isomorphe Substruktur enthalten. Dies gewährleistet dann, dass gilt:

φ_M hat ein endliches Modell $\Longrightarrow$
$\mathcal{A}_M$ ist endlich $\Longrightarrow$
M hält bei Eingabe ε.

Außerdem konstruieren wir φ_M so, dass auch gilt: $\mathcal{A}_M \models \varphi_M$. Dies gewährleistet dann, dass gilt:
M hält bei Eingabe ε $\Longrightarrow$
$\mathcal{A}_M$ ist endlich $\Longrightarrow$
φ_M hat ein endliches Modell.

Insgesamt gilt dann also:

φ_M hat ein endliches Modell $\Longleftrightarrow$
M hält bei Eingabe ε,

und wir sind dann fertig mit dem Beweis.

<u>Zur Konstruktion von φ_M</u>:

Klar: Die Struktur $\mathcal{A}_M$ erfüllt die Punkte (1)-(4).

Punkt (1) wird durch folgende Formel beschrieben:

$$\varphi_{<,succ,0} :=$$

$$\forall x \forall y \forall z \Big(\big((x<y \wedge y<z) \rightarrow x<z \big) \quad \text{transitiv}$$

$$\wedge \; (x<y \rightarrow \neg y<x) \quad \text{antisymmetrisch}$$

$$\wedge \; (x<y \vee y<x \vee y=x) \quad \text{konnex}$$

$$\wedge \; (0=x \vee 0<x) \quad \text{0 ist kleinstes Element}$$

$$\wedge \; \big(succ(x,y) \leftrightarrow (x<y \wedge \neg \exists u (x<u \wedge u<y)) \big) \Big) \quad \text{succ ist Nachfolger-Relation}$$

In jedem Modell $\mathcal{A}$ von $\varphi_{<,succ,0}$

können wir die Elemente $a_0, a_1, a_2, a_3, \dots$, für die gilt

$a_0 = 0^{\mathcal{A}}$,

$(a_0, a_1) \in succ^{\mathcal{A}}$,

$(a_1, a_2) \in succ^{\mathcal{A}}$,

$(a_2, a_3) \in succ^{\mathcal{A}}$,

$\dots$

mit den natürlichen Zahlen $0, 1, 2, 3, \dots$ identifizieren.

Die folgende Formel erzwingt in ihren Modellen, dass die Variablen $z_0, z_1, \dots, z_s$ mit diesen Elementen $a_0, a_1, \dots, a_s$ (also im Grunde mit den natürlichen Zahlen $0, 1, \dots, s$) belegt werden:

$$\varphi_{zahlen}(z_0, z_1, \dots, z_s) :=$$
$$z_0 = 0 \ \wedge \ \bigwedge_{i=1}^{s} succ(z_{i-1}, z_i)$$

<u>Zur Erinnerung</u>: $s = \max\{s_Q, s_\Gamma\}$, mit $Q = \{0, 1, \dots, s_Q\}$ und $\Gamma = \{0, 1, \dots, s_\Gamma\}$.

Der $FO[\sigma]$-Satz φ_M wird nun folgendermaßen gewählt:

$$\varphi_M :=$$

$$\varphi_{<,succ,0} \wedge \exists z_0 \cdots \exists z_s \Big($$

$$\varphi_{Zahlen}(z_0, \ldots, z_s) \wedge$$

$$\varphi_{Band} \wedge \varphi_{Kopf} \wedge \varphi_{Zustand} \wedge$$

$$\varphi_{Start} \wedge \varphi_{Schritt} \Big),$$

wobei die Formeln der letzten beiden Zeilen wie folgt gewählt sind:

- φ_{Band} besagt, dass zu jedem Zeitpunkt auf jeder Bandposition genau ein Symbol des Arbeitsalphabets $\Gamma = \{0, \ldots, s_\Gamma\}$ steht.

$$\varphi_{Band} := \forall x \forall y \exists z \Big(B(x,y,z) \wedge \Big(\bigvee_{i=0}^{s_\Gamma} z = z_i \Big) \wedge$$

$$\forall z' \big(B(x,y,z') \rightarrow z' = z \big) \Big)$$

- $\varphi_{Zustand}$ besagt, dass M zu jedem Zeitpunkt in genau einem Zustand aus $Q = \{0, 1, \ldots, s_Q\}$ ist:

$$\varphi_{Zustand} := \forall x \, \exists z \left(Z(x,z) \wedge \left(\bigvee_{i=0}^{s_Q} z = z_i \right) \wedge \forall z' \left(Z(x,z') \rightarrow z' = z \right) \right)$$

- φ_{Kopf} besagt, dass der Schreib-/Lesekopf von M zu jedem Zeitpunkt auf genau einer Bandposition steht:

$$\varphi_{Kopf} := \forall x \, \exists y \left(K(x,y) \wedge \forall y' \left(K(x,y') \rightarrow y' = y \right) \right)$$

- φ_{Start} besagt, dass M zum Zeitpunkt 0 in der Startkonfiguration $C_0(\varepsilon)$ bei Eingabe des leeren Worts ist, d.h. sie ist im Startzustand $q_0 = 0$, ihr Schreib-/Lesekopf steht auf Bandposition 0, und auf jeder Bandposition steht das Blank-Symbol $\Box = 0$. Somit wählen wir:

$$\varphi_{Start} := Z(0,0) \wedge K(0,0) \wedge \forall y \, B(0,y,0)$$

- φ_{Schritt} besagt für jeden Zeitpunkt t:

  Falls M zum Zeitpunkt t nicht in einem Endzustand ist, so ist sie zum Zeitpunkt $t' := t+1$ in einem laut Übergangsrelation zulässigen Zustand q', hat das entsprechende Symbol auf's Band geschrieben, den Kopf an die richtige Stelle bewegt und die Beschriftung aller anderen Bandpositionen nicht verändert.
  Somit wählen wir:

$$
\begin{aligned}
\varphi_{\text{Schritt}} :=\ & \forall t\, \forall p \bigwedge_{q \in Q\setminus F}\ \bigwedge_{\gamma \in \Gamma} \Big(\big(K(t,p) \wedge Z(t,z_q) \wedge B(t,p,z_\gamma) \big) \rightarrow \\
& \qquad \exists t'\, \exists p' \Big(succ(t,t') \wedge K(t',p') \wedge \\
& \forall p'' \Big(p''=p \vee \bigwedge_{\gamma'' \in \Gamma} \big(B(t',p'',z_{\gamma''}) \leftrightarrow B(t,p'',z_{\gamma''}) \big) \Big) \wedge \\
& \Big(\bigvee_{\substack{q',\gamma',m: \\ (q,\gamma,q',\gamma',m) \in \Delta}} \big(Z(t',z_{q'}) \wedge B(t',p,z_{\gamma'}) \wedge \chi_m(p,p') \big) \Big) \Big) \Big)
\end{aligned}
$$

wobei die Formel $\chi_m(p,p')$ die Kopfbewegung für $m \in \{-1,0,1\}$ beschreibt, d.h.:

$\chi_0(p,p') := p'=p$, $\chi_1(p,p') := succ(p,p')$, $\chi_{-1}(p,p') := succ(p',p)$.

Die dritte Zeile von $\varphi_{schritt}$ besagt, dass an allen Bandpositionen $p'' \neq p$ die Beschriftung zum Zeitpunkt t' dieselbe ist wie zum Zeitpunkt t.

Zeile vier besagt, dass beim Übergang von Zeitpunkt t zum Zeitpunkt t' der Zustand, die Bandbeschriftung an Position p und die neue Kopfposition p' entsprechend der Übergangsrelation Δ gewählt wird.

Wir sind nun fertig mit der Konstruktion der Formel φ_M. Gemäß dieser Konstruktion gilt:

- $\mathcal{A}_M \models \varphi_M$ und
- in jeder σ-Struktur $\mathcal{A}$ mit $\mathcal{A} \models \varphi_M$ gibt es Elemente $a_0, a_1, a_2, \ldots$, die den natürlichen Zahlen $0, 1, 2, \ldots$ entsprechen, und schränkt man $\mathcal{A}$ ein auf das Teiluniversum $\{a_i : i \in A_M\}$, so erhält man eine Struktur, die isomorph zu $\mathcal{A}_M$ ist.

Außerdem sieht man leicht, dass es einen Algorithmus gibt, der bei Eingabe einer DTM M den $\mathrm{FO}[\sigma]$-Satz φ_M konstruiert. Das Halteproblem H_ε kann dann dadurch getestet werden, dass man φ_M auf endliche Erfüllbarkeit testet. Widerspruch zu Satz 1.6. $\square$

Bemerkung 1.10:

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

Daraus folgt dann natürlich auch, dass der Satz von Trakhtenbrot für jede Signatur gilt, die mindestens ein Relationssymbol der Stelligkeit ≥ 2 enthält.

Andererseits werden wir in einem späteren Kapitel, unter Verwendung von Lokalitätsresultaten zeigen, dass für jede funktionenfreie Signatur σ, deren Relationssymbole alle die Stelligkeit 1 haben, das endliche Erfüllbarkeitsproblem für $FO[\sigma]$ entscheidbar ist.

Bemerkung 1.11:

Alternativ zum Halteproblem H_E kann man auf Grund des Satzes von Trakhtenbrot auch das endliche Erfüllbarkeitsproblem für $FO[\sigma]$ als Grundlage für Reduktionen nutzen, mit denen man die Unentscheidbarkeit bestimmter Probleme nachweist. Beispiele dazu werden in den Übungen betrachtet.