Rückblick §2: Mengenlehre

Axiomensystem

Zermelo - Fränkel (ZF)

- Extensionalität
- Aussonderung
- Paarmenge
- Vereinigung
- Potenzmenge
- Ersetzung
- Fundierung
- Unendlichkeit

Choice: (C)

- Auswahlaxiom

Nun: Entwickele Mathematik in ZFC

Für $n \in \mathbb{N}$ definiere $\underline{n} = \{\underline{0}, \dots, \underline{n-1}\}$

Def: Natürliche Zahl (transitive Menge, durch $\in$ linear geordnete, jede nicht-leere TM hat Min & Max).

$\omega = \{x : x \text{ ist natürliche Zahl}\}$ ist eine Menge.

$\rightsquigarrow$ es gilt Induktion & der Rekursionssatz, insbes. sind $+, \cdot : \omega \times \omega \to \omega$ Funktionen im Sinne der ML

Def: Ordinalzahl (transitiv, durch $\in$ lin. geordnet)

$On = \{x : x \text{ ist Ordinalzahl}\}$ ist keine Menge.

$\rightsquigarrow$ dennoch gelten Induktion & Rekursionssatz

↑ Fallunterscheidung: $\underline{0}$, $\alpha = \beta + 1$, α Limeszahl

$On = \{WO\text{-Typen}\}$

In ZF sind äquivalent: $\left\{ \begin{array}{l} \text{Auswahlaxiom} \\ \text{WO-Satz} \\ \text{Zornsches Lemma} \end{array} \right.$

Kardinalzahl ($\alpha \in On$ mit $\alpha = |\alpha|$)

WO-Satz $\Rightarrow$ jede Menge ist gleichmächtig zu einer Kardinalzahl.

Cantor: Es gibt keine größte Kard.zahl.

$\rightsquigarrow$ erhalte $\aleph$-Hierarchie.

Metamathematik:

Kodiere L_{Me}-Fmln $\mathfrak{A}$ durch $\ulcorner \mathfrak{A} \urcorner$

Führe Beweisbarkeitsprädikat $Bew(\ulcorner \mathfrak{A} \urcorner)$ ein.

$CON_{ZFC} := \neg Bew(\ulcorner F \urcorner)$ $\quad$ F L_{Me}-Fml, deren Negation allg. gültig ist.

2 GUS: ZFC kons. $\Rightarrow$ $ZFC \nvdash CON_{ZFC}$

1 GUS: ZFC kons. $\Rightarrow$ ex. L_{Me}-Aussage R.

$ZFC \nvdash R$, $ZFC \nvdash \neg R$.

§3 Rekursionstheorie

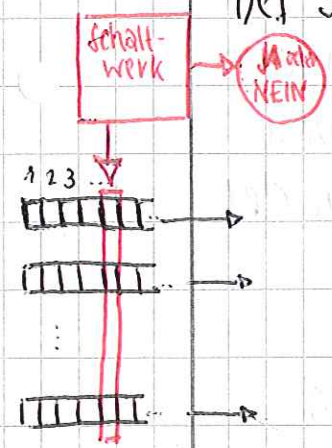
Idee: $f: \mathbb{N}^n \to \mathbb{N}$ heißt TM-berechenbar, wenn es eine TM gibt, die f berechnet.
← Modell eines Computers

Fakt: Sei $f: \mathbb{N}^n \to \mathbb{N}$ eine Funktion. Dann sind äquivalent:
(1.) f ist Turing-berechenbar
(2.) f ist in einer 'üblichen' Programmiersprache berechenbar (etwa: C, C++, Java, Pascal, R, Haskell, ..)

Church'sche These: Jede intuitiv berechenbare Funktion $f: \mathbb{N}^n \to \mathbb{N}$ ist Turing-berechenbar.

Ziele: • Definiere TM etc.
• Zeige $f: \mathbb{N}^n \to \mathbb{N}$ berechenbar gdw. $\underbrace{\text{rekursiv}}_{\text{Mathematische Beschreibung}}$.

§3.1 Turingmaschinen und rekursive Funktionen



Def 3.1. Eine Turingmaschine M wird durch die folgenden Daten gegeben:
- eine endl. Anzahl von Bändern $B_1, B_2, \ldots$ horizontal angeordnet, jedes nach links beschränkt und nach rechts unbeschränkt. Jedes Band ist unterteilt in Kästchen, diese werden durch $\mathbb{N}_{>0}$ von links nach rechts durchnummeriert.
Die Bänder sind so angeordnet, dass Kästchen mit der gleichen Nummer ~~xxx~~ vertikal übereinander liegen.
- ein Lese-/Schreibkopf, der Zeichen (Symbole) aus den Kästchen des Bandes auslesen, löschen oder überschreiben kann.

Der Kopf bewegt sich horizontal und ist stets über einer (vertikalen) Spalte, er verändert alle Einträge der Spalte simultan.
Die Zeichenmenge (oder das Alphabet) ist $S = \{\$, 1, b\}$
b heißt "blank" oder das leere Zeichen.
Hinzu kommen die folgenden Daten, die spezifisch zu M gehören
- $n = n(M) \in \mathbb{N}_{>0}$ die Anzahl der Bänder
- eine endl. Menge Q von Zuständen. Q enthält ~~xxx~~ einen Startzustand q_I und einen akzeptierenden Zustand q_F mit $q_I \neq q_F$.
- eine Funktion $M: S^n \times Q \to S^n \times Q \times \{-1, 0, 1\}$, die Übergangsfunktion von M.

Wie arbeitet die TM M?
- zu jedem Zeitpunkt ~~xxx~~ $t \in \mathbb{N}$ ist M in einem Zustand $q \in Q$.
- M arbeitet zu jedem Zeitpunkt durch Zustandswechsel, das Löschen und das Schreiben von Symbolen auf das Band und durch Bewegen des Kopfes.

Dabei gelten die folgenden Regeln:
(1) Zum Zeitpunkt $t = 0$ ist M im Anfangszustand und der Kopf ruht auf der ersten Spalte
(2) Zu jedem Zeitpunkt t liest M die Zeichen $(s_1, \ldots, s_n) \in S^n$ aus, die unter seinem Kopf stehen, und die Übergangsfkt gibt an, was zu tun ist. Wenn M in Zustand q ist und $(s_1, \ldots, s_n)$ liest, und $M(\bar{s}, q) = (\bar{s}', q', \varepsilon)$

dann löscht der Kopf $\bar{s}$, schreibt $\bar{s}'$, bewegt sich horizontal um ε und M wechselt in Zustand q'. ~~und~~ Dann wechselt der Zeitpunkt zu $t+1$.

(3.) Wenn sich M im Zustand q_F befindet, hört M auf zu arbeiten.

Gültige Eingabe:

- Zum Zeitpunkt $t=0$ steht \$ in allen Einträgen in der ersten Spalte und nur dort.
- In jedem Kästchen steht ein Zeichen aus S, und nur endl. viele Kästchen sind nicht-leer (d.h. enthalten \$ oder 1).

(Diese Bedingungen bleiben während der gesamten ~~gesamtenten~~ Berechnung wahr)

Weitere Nebenbedingungen:

- für jedes $\bar{s} \in S^n$ gilt $M(\bar{s}, q_F) = (\bar{s}, q_F, 0)$
- Der Kopf kann \$ nicht löschen (\$ markiert den Beginn eines jeden Bandes) oder ein Symbol, was nicht \$ ist, nicht mit \$ überschreiben:
  - für jedes $q \in Q$ gilt:
    $M((\$, \ldots, \$), q) = ((\$, \ldots, \$), q, \varepsilon)$ für ein $\varepsilon \in \{0, 1\}$
  - Wenn $\bar{s} \neq (\$, \ldots, \$)$ dann gilt
    $M(\bar{s}, q) = (\bar{s}', q', \varepsilon)$ mit $s_i' \neq \$$ f.a. i.

Bem: Unsere TM sind deterministisch (jeder Schritt folgt in eindl. Weise aus der vorherigen Berechnung)

Def 3.2: (1.) Ein Band repräsentiert (zu einem gegebenen Zeitpunkt) eine natürliche Zahl m, wenn der Bandinhalt $(\$, \underbrace{1, \ldots, 1}_{m\text{-mal}}, b, b, b, \ldots)$ ist.

(2.) Eine partielle Funktion von $\mathbb{N}^p$ nach $\mathbb{N}$ ist ein Tupel (A, f), mit $A \subseteq \mathbb{N}^p$ und $f: A \to \mathbb{N}$. Schreibe $A = dom(f)$ und $\mathcal{F}_p^*$ für die Menge all dieser Paare.

(3.) Eine TM $\mathcal{M}$ berechnet $f \in \mathcal{F}_p^*$ wenn $n(\mathcal{M}) \geq p+1$ gilt und f.a. $\bar{m} \in \mathbb{N}^p$, ~~we~~ gilt: Wenn $\mathcal{M}$ auf dem Input startet, bei dem die Bänder $B_1, \ldots, B_p$ die Zahlen $m_1, \ldots, m_p$ repräsentieren, und B_i für $i > p$ die Zahl 0 repräsentiert, dann

(i) falls $\bar{m} \in dom(f)$ stoppt $\mathcal{M}$ nach endl. Zeit und die Bänder von $\mathcal{M}$ repräsentieren $(m_1, \ldots, m_p, f(\bar{m}), 0, \ldots, 0)$ (in dieser Reihenfolge!)

(ii) falls $\bar{m} \notin dom(f)$, stoppt $\mathcal{M}$ nie (d.h. $\mathcal{M}$ wechselt nie in Zustand q_1).

(4.) Eine partielle Fkt f heißt Turing-berechenbar, wenn es eine TM $\mathcal{M}$ gibt, die f berechnet ($f \in \mathcal{F}_p^*$ für ein $p \in \mathbb{N}$)

Lemma 3.3: Die Funktionen $S: \mathbb{N} \to \mathbb{N}, x \mapsto x+1$, $C_0^0: \mathbb{N}^0 \to \mathbb{N}, C_0^0 = 0$ und ~~Pi~~ $P_i^n: \mathbb{N}^n \to \mathbb{N}$, $(m_1, \ldots, m_n) \mapsto m_i$ für alle $n \in \mathbb{N}_{>0}$, $1 \leq i \leq n$ sind TM-berechenbar.

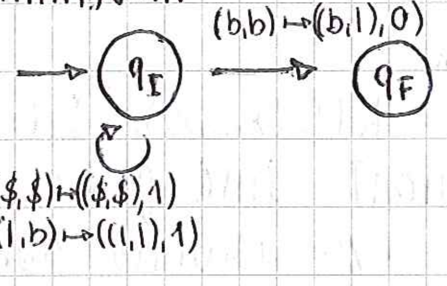
Bew: · C: wird durch eine TM $\mathcal{M}$ mit einem Band berechnet, Zustandsmenge $Q = \{q_I, q_F\}$ und Übergangsfkt. $M(\$, q_I) = (\$, q_F, 0)$ ('relevanter Teil')
(setze etwa fort durch $M(1, q_I) = (1, q_I, 0)$ und $M(b, q_I) = (b, q_I, 0)$)

· f wird durch TM $\mathcal{M}$ mit zwei Bändern berechnet, Zustandsmenge $Q = \{q_I, q_F\}$ und Übergangsfkt.
~~[illegible]~~ $M((\$,\$), q_I) = ((\$,\$), q_I, 1)$,
$M((1,b), q_I) = ((1,1), q_I, 1)$, $M((b,b), q_I) = ((b,1), q_F, 0)$

⌈ Alternativer Beweis (auch okay): Modulbeschreibung
- Lese aktuelle ~~[illegible]~~ Spalte. Falls oberer Eintrag \$, rücke Lesekopf nach rechts.
Falls ~~aktuelles~~ oberer Eintrag 1, schreibe (1,1) und rücke Lesekopf nach rechts.
Falls oberer Eintrag b, schreibe (b,1) und wechsele in akz. Zustand.
⌊ ☒

(Pi": Übung!)

Diagrammform



Anmerkung: · Sowohl Modulbeschreibungen als auch (Fluss-) Diagramme können zur Beschreibung von TM benutzt werden!
· Es gibt noch viele weitere Möglichkeiten, TM zu definieren, bspw. 1-Band oder Band durch $\mathbb{Z}$ nummeriert. Alle berechnen die gleichen Fkt!
(siehe BT-Vorlesung)