

Intuitive und Turing-Berechenbarkeit

Prof. Dr. David Sabel

LFE Theoretische Informatik



Letzte Änderung der Folien: 19. Juni 2022

Historie

- Berühmte Mathematiker / Informatiker versuchten in den 1930er Jahren den Begriff der Berechenbarkeit zu formalisieren
- dafür entwarfen sie verschiedene Modelle
- insbesondere sind zu nennen:
 - Alan Turing (Turingmaschine)
 - Alonzo Church (Lambda-Kalkül)

Intuitive Berechenbarkeit

Motivation / Fragen

- Was **kann** mit einem Computerprogramm berechnet werden?
- Was **kann nicht** mit einem Computerprogramm berechnet werden?
- Aus der (Programmier-)Erfahrung:

Man hat ein gewisses Gefühl dafür, was berechnet werden kann (und was nicht).

- Das ist der intuitive Begriff der Berechenbarkeit.
- Wie beweist man, dass etwas nicht berechnet werden kann?

Diese Frage ist auch von praktischem Nutzen:
Suche nach „passendem“ Algorithmus ist sinnlos.

Berechenbare Funktion

Eine Funktion $f : \mathbb{N}^k \rightarrow \mathbb{N}$ nennen wir **berechenbar**, wenn

- es gibt einen Algorithmus einer modernen Programmiersprache, der f berechnet:
 - Bei Eingabe (n_1, \dots, n_k) stoppt der Algorithmus nach endlich vielen Berechnungsschritten und liefert den Wert von $f(n_1, \dots, n_k)$ als Ausgabe.
 - Wenn $f(n_1, \dots, n_k)$ undefiniert ist (f ist also eine partielle Funktion), dann stoppt der Algorithmus nicht.

Beispiele

Der Algorithmus

Eingabe: Zahl $n \in \mathbb{N}$

Beginn

```
┌ solange true tue
│   └ skip
```

berechnet $f_1 : \mathbb{N} \rightarrow \mathbb{N}$ mit $f_1(x) = \text{undefiniert}$ für alle x

Der Algorithmus

Eingabe: Zahlen $n_1, n_2 \in \mathbb{N}$

Beginn

```
┌ hilf := n1 + n2;
│   └ return hilf
```

berechnet die Funktion $f_2 : (\mathbb{N} \times \mathbb{N}) \rightarrow \mathbb{N}$ mit $f_2(x, y) = x + y$.

f_1 und f_2 sind daher berechenbar

Beispiele (2)

$$f_3(n) = \begin{cases} 1, & \text{falls } n \text{ ein Präfix der Ziffern der Dezimalzahl-} \\ & \text{darstellung von } \pi \text{ ist} \\ 0, & \text{sonst} \end{cases}$$

Z.B. gilt

- $f_3(31) = 1$ und $f_3(314) = 1$
- $f_3(2) = 0$ und $f_3(315) = 0$

Ist f_3 berechenbar?

Ja: Sei n eine k -stellige Zahl. Es gibt Algorithmen, die die ersten k Stellen von π berechnen. Danach kann man vergleichen.

Beispiele (3)

$$f_4(n) = \begin{cases} 1, & \text{falls } n \text{ ein Teilwort der Ziffern} \\ & \text{der Dezimalzahldarstellung von } \pi \text{ ist} \\ 0, & \text{sonst} \end{cases}$$

Ist f_4 berechenbar?

Unklar. Es gibt die Vermutung, dass jede x -beliebige Ziffernfolge irgendwann als Folge in π auftaucht, aber die Frage ist bisher ungelöst.

Beispiele (4)

$$f_5(n) = \begin{cases} 1, & \text{falls die Dezimaldarstellung von } \pi \text{ das Wort } 3^m \\ & \text{mit } m \geq n \text{ als Teilwort besitzt.} \\ 0, & \text{sonst} \end{cases}$$

Ist f_5 berechenbar?

Ja:

- Entweder: $f_5(n) = 1$ für alle n
- Oder: Es gibt m_0 , sodass π 3^{m_0} als Teilwort hat, aber alle Teilworte 3^m mit $m > m_0$ nicht mehr besitzt.

$$\text{Dann ist } f_5(n) = \begin{cases} 1, & \text{falls } n \leq m_0 \\ 0, & \text{falls } n > m_0 \end{cases}$$

- Egal, welcher Fall zutrifft, wir können für beide Fälle Algorithmen angeben, die f_5 berechnen.

Beachte: Unsere Definition von Berechenbarkeit ist **nicht konstruktiv**:

Wir müssen keinen Algorithmus liefern, sondern nur einen Beweis, dass der Algorithmus existiert.

Beispiele (5)

$$f_6(n) = \begin{cases} 1, & \text{falls deterministische LBAs genau die gleichen} \\ & \text{Sprachen erkennen wie nichtdeterministische LBAs} \\ 0, & \text{sonst} \end{cases}$$

Ist f_6 berechenbar?

Ja: Entweder ist $f_6(x) = 1$ oder $f_6(x) = 0$.
Beide Funktionen sind berechenbar.

(Unabhängig davon, ob das 1. LBA Problem eine positive oder negative Lösung hat)

Beispiele (6)

$$f^r(n) = \begin{cases} 1, & \text{falls } n \text{ ein Präfix der Ziffern der} \\ & \text{Dezimalzahldarstellung von } r \text{ ist} \\ 0, & \text{sonst} \end{cases}$$

Ist f^r für jedes $r \in \mathbb{R}$ berechenbar?

Nein: Wir bräuchten genauso viele verschiedene Algorithmen wie es reelle Zahlen gibt.
Es gibt nur abzählbar viele Algorithmen einer Programmiersprache,
aber überabzählbar viele reelle Zahlen

Churchsche These

Im folgenden untersuchen wir (nur in FSK) Modelle zur Berechenbarkeit

- Turingmaschinen
- WHILE-Programme
- GOTO-Programme
- μ -rekursive Funktionen

Resultat: Alle führen zum selben Begriff der Berechenbarkeit.

Churchsche These:

Die Klasse der Turingberechenbaren (äquivalent WHILE-berechenbaren, GOTO-berechenbaren, μ -rekursiven) Funktionen stimmt genau mit der Klasse der intuitiv berechenbaren Funktionen überein.

Die Churchsche These kann man nicht beweisen, da der Begriff „intuitiv berechenbar“ nicht formal gefasst werden kann.

Turingmaschinen: Wiederholung

- Ein Turingmaschine ist ein 7-Tupel $(Z, \Sigma, \Gamma, \delta, z_0, \square, E)$ mit Zuständen Z , Eingabealphabet Σ , Bandalphabet $\Gamma \supset \Sigma$, Blank-Symbol \square , Startzustand z_0 , Endzuständen $E \subseteq Z$, und Überföhrungsfunktion δ .
- DTM: $\delta : (Z \times \Gamma) \rightarrow (Z \times \Gamma \times \{L, R, N\})$
- NTM: $\delta : (Z \times \Gamma) \rightarrow \mathcal{P}(Z \times \Gamma \times \{L, R, N\})$
- TM-Konfiguration $a_1 \cdots a_m z a_{m+1} \cdots a_n$, wobei $a_1 \cdots a_n \in \Gamma^*$ der entdeckte Teil des Bands, TM ist in Zustand z und Kopf ist unter a_{m+1} .

Turingberechenbarkeit

Definition (Turingberechenbarkeit)

Sei $bin(n)$ die Binärdarstellung von $n \in \mathbb{N}$.

Eine Funktion $f: \mathbb{N}^k \rightarrow \mathbb{N}$ heißt **Turingberechenbar**, falls es eine (deterministische) Turingmaschine $M = (Z, \Sigma, \Gamma, \delta, z_0, \square, E)$ gibt, so dass für alle $n_1, \dots, n_k, m \in \mathbb{N}$ gilt:

$$f(n_1, \dots, n_k) = m \quad \text{g.d.w.} \\ z_0 bin(n_1) \# \dots \# bin(n_k) \vdash^* \square \dots \square z_e bin(m) \square \dots \square \text{ mit } z_e \in E.$$

Eine Funktion $f: \Sigma^* \rightarrow \Sigma^*$ heißt **Turingberechenbar**, falls es eine (deterministische) Turingmaschine $M = (Z, \Sigma, \Gamma, \delta, z_0, \square, E)$ gibt, so dass für alle $u, v \in \Sigma^*$ gilt

$$f(u) = v \text{ g.d.w. } z_0 u \vdash^* \square \dots \square z_e v \square \dots \square \text{ mit } z_e \in E.$$

Konsequenzen

Eine Konsequenz der Definition ist:

Falls $f(n_1, \dots, n_k)$ bzw. $f(u)$ undefiniert ist, dann kann die Maschine in eine Endlosschleife gehen.

Wir nehmen von nun an sogar an:

Die Maschine geht in diesem Fall stets in eine Endlosschleife.

Beispiele

Nachfolgerfunktion

Die Funktion $f(x) = x + 1$ für alle $x \in \mathbb{N}$ ist Turingberechenbar. Wir haben eine entsprechende Turingmaschine bereits angegeben.

Identitätsfunktion

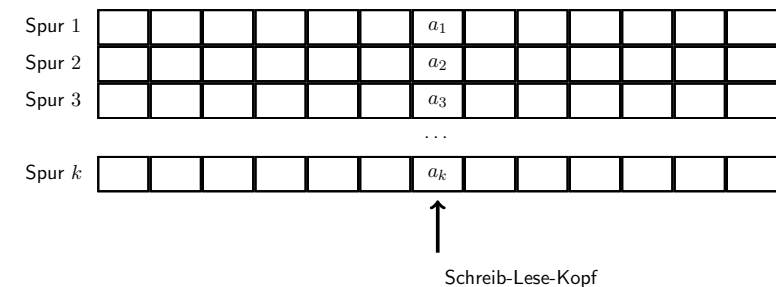
Die Funktion $f(x) = x$ für alle $x \in \mathbb{N}$ ist Turingberechenbar: Für die Turingmaschine $M = (\{z_0\}, \{0, 1, \#\}, \{0, 1, \#\square\}, \delta, z_0, \square, \{z_0\})$ mit $\delta(z_0, a) = (z_0, a, N)$ für alle $a \in \{0, 1, \#, \square\}$ gilt: $z_0 bin(n) \vdash^* z_0 bin(n)$ für alle $n \in \mathbb{N}$.

Überall undefinierte Funktion

Die Funktion $f(x) = \perp$ für alle x ist Turingberechenbar, da die TM $M = (\{z_0\}, \{0, 1, \#\}, \{0, 1, \#, \square\}, \delta, z_0, \square, \emptyset)$ mit $\delta(z_0, a) = (z_0, a, N)$ für keine Eingabe akzeptiert (sondern stets in eine Endlosschleife geht).

Mehrspuren-Turingmaschinen (1)

Erweiterung: Das Band hat k -Spuren:



Mehrspuren-Turingmaschinen (2)

Definition (Mehrspuren-Turingmaschine)

Eine **k -Spuren-Turingmaschine** ($k \in \mathbb{N}_{>0}$) ist ein 7-Tupel $(Z, \Sigma, \Gamma, \delta, z_0, \square, E)$ mit

- Z ist eine endliche Menge von **Zuständen**,
- Σ ist das (endliche) **Eingabealphabet**,
- $\Gamma \supset \Sigma$ ist das (endliche) **Bandalphabet**,
- δ ist die **Zustandsüberföhrungsfunktion**:
 - für eine DTM: $\delta : (Z \times \Gamma^k) \rightarrow Z \times \Gamma^k \times \{L, R, N\}$
 - für eine NTM: $\delta : (Z \times \Gamma^k) \rightarrow \mathcal{P}(Z \times \Gamma^k \times \{L, R, N\})$
- $z_0 \in Z$ ist der **Startzustand**,
- $\square \in \Gamma \setminus \Sigma$ ist das **Blank-Symbol** und
- $E \subseteq Z$ ist die Menge der **Endzustände**.

Berechenbarkeit: Ein- und Ausgabe auf der ersten Spur.

Mehrspuren-Turingmaschinen (3)

Berechenbarkeit: Ein- und Ausgabe auf der ersten Spur.

Satz

Jede Mehrspuren-Turingmaschine kann auf einer 1-Band-Turingmaschine simuliert werden.

Beweis: Konstruktion der 1-Band-TM mit einer Spur:

- Verwende als Bandalphabet $\Gamma \cup \Gamma^k$
- Eingabealphabet Σ und Blank-Symbol \square .
- Aus Eingabe w aus Σ^* erzeugt die TM die Mehrspurendarstellung: Ersetze $a \in \Sigma$ durch k -Tupel $(a, \square, \dots, \square)$.
- Anschließend wird die Mehrspurenmaschine simuliert
- Nach Akzeptanz der Mehrspurenmaschine: Erzeuge 1-Spuren-Darstellung, d.h. ersetze alle (a_1, \dots, a_k) durch a_1 . \square

Beispiel einer Mehrspurenmaschine (1)

- TM, die $\{w cw \mid w \in \{a, b\}^+\}$ erkennt.
- Wir konzentrieren uns auf die 2-Spurendarstellung, daher: TM, die $\{w(c, \square)w \mid w \in \{(a, \square), (b, \square)\}^+\}$ erkennt

Ideen:

- Eingabe wcw auf Spur 1 wird nur gelesen nicht verändert.
- Auf Spur 2 wird nur \square und \checkmark zum Markieren von Zeichen auf Spur 1 verwendet.
- Markieren: Erst ein Zeichen im linken w , dann selbes Zeichen im rechten w
- Zustände $Z = \{z_0, z_{1a}, z_{1b}, z_{2a}, z_{2b}, z_3, \dots, z_9\}$
 $z_{1a}, z_{1b}, z_{2a}, z_{2b}$ „speichern“ das gelesene Zeichen (a oder b).
 - z_0 ist der Startzustand.
 - z_8 ist der einzige akzeptierende Zustand.
 - z_9 ist Müllzustand (zum Verwerfen)

Beispiel einer Mehrspurenmaschine (2)

Übergangsfunktion δ

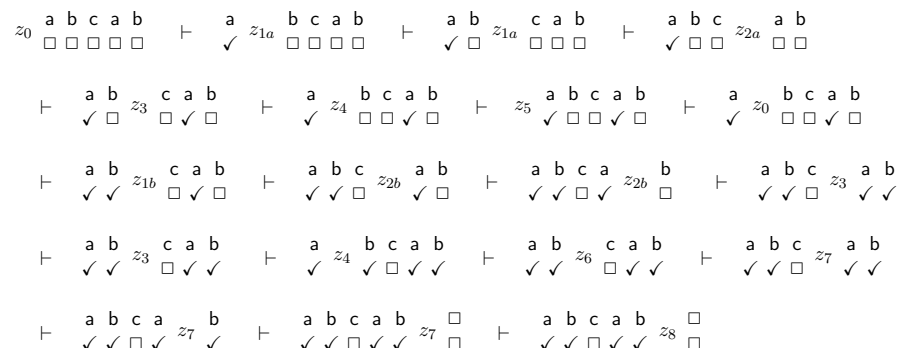
- $\delta(z_0, (s, \square)) = (z_{1s}, (s, \checkmark), R)$ für $s \in \{a, b\}$: markiere linkstes unmarkiertes Zeichen s im linken w , speichere s in z_{1s} , Suche nach s im rechten w beginnt.
- $\delta(z_{1s}, (s', \square)) = (z_{1s}, (s', \square), R)$ für $s, s' \in \{a, b\}$: laufe nach rechts zum c
- $\delta(z_{1s}, (c, \square)) = (z_{2s}, (c, \square), R)$ mit $s \in \{a, b\}$: c wurde erreicht
- $\delta(z_{2s}, (s', \checkmark)) = (z_{2s}, (s', \checkmark), R)$ mit $s, s' \in \{a, b\}$: suche erstes unmarkiertes Symbol im rechten w .
- $\delta(z_{2s}, (s, \square)) = (z_3, (s, \checkmark), L)$ mit $s \in \{a, b\}$: richtiges unmarkiertes Zeichen im rechten w .
- $\delta(z_3, (s, \checkmark)) = (z_3, (s, \checkmark), L)$ mit $s \in \{a, b\}$: nach links laufen zum c .
- $\delta(z_3, (c, \square)) = (z_4, (c, \square), L)$ c von rechts wieder erreicht.
- ...

Beispiel einer Mehrspurenmaschine (3)

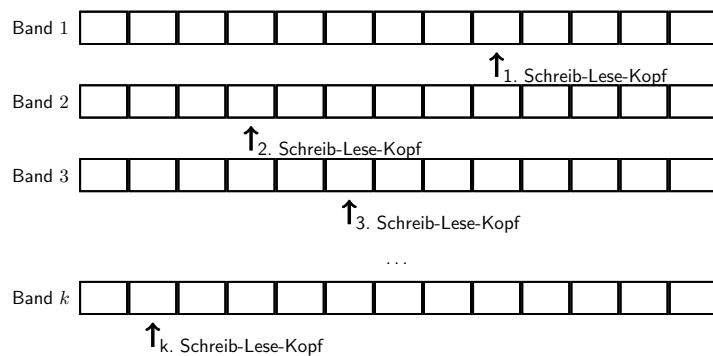
- ...
- $\delta(z_4, (s, \square)) = (z_5, (s, \square), L)$ mit $s \in \{a, b\}$: links vom c kein markiertes Zeichen: zu z_5
- $\delta(z_4, (s, \checkmark)) = (z_6, (s, \square), R)$ mit $s \in \{a, b\}$: links vom c ist markiertes Zeichen: Prüfe, dass alle Zeichen im rechten w markiert sind (mit z_6).
- $\delta(z_5, (s, \square)) = (z_5, (s, \square), L)$ mit $s \in \{a, b\}$: suche erstes markiertes Zeichen im linken w
- $\delta(z_5, (s, \checkmark)) = (z_0, (s, \checkmark), R)$ mit $s \in \{a, b\}$: erstes markiertes Zeichen im linken w gefunden, gehe zu z_0
- $\delta(z_6, (c, \square)) = (z_7, (c, \square), R)$: suche im rechten w nach unmarkierten Zeichen
- $\delta(z_7, (s, \checkmark)) = (z_7, (s, \checkmark), R)$ für $s \in \{a, b\}$: suche im rechten w nach unmarkierten Zeichen
- $\delta(z_7, (\square, \square)) = (z_8, (\square, \square), N)$: alle Zeichen im rechten w markiert, akzeptiere in z_8
- $\delta(z_8, (s, t)) = (z_8, (s, t), N)$ für $s \in \{a, b, c\}$, $t \in \{\square, \checkmark\}$ verbleibe akzeptierend.
- $\delta(z_i, (s, t)) = (z_9, (s, t), N)$ für alle anderen Fälle verbleibe oder wechsele in den verwerfenden Zustand.

Beispiel einer Mehrspurenmaschine (4)

Ein Lauf der Turingmaschine für das Wort $abcab$ ist:



Mehrbandmaschinen



Schreib-Lese-Köpfe bewegen sich unabhängig!

Mehrbandmaschinen (2)

Definition (Mehrband-Turingmaschine)

Eine k -Band-Turingmaschine (für $k \in \mathbb{N}_{>0}$) ist ein 7-Tupel $(Z, \Sigma, \Gamma, \delta, z_0, \square, E)$ mit

- Z ist eine endliche Menge von Zuständen,
- Σ ist das (endliche) Eingabealphabet,
- $\Gamma \supset \Sigma$ ist das (endliche) Bandalphabet,
- δ ist die Zustandsübergangsfunktion
 - für eine DTM: $\delta : (Z \times \Gamma^k) \rightarrow (Z \times \Gamma^k \times \{L, R, N\}^k)$
 - für eine NTM: $\delta : (Z \times \Gamma^k) \rightarrow \mathcal{P}(Z \times \Gamma^k \times \{L, R, N\}^k)$
- $z_0 \in Z$ ist der Startzustand,
- $\square \in \Gamma \setminus \Sigma$ ist das Blank-Symbol
- $E \subseteq Z$ ist die Menge der Endzustände.

Berechnung: Eingabe auf dem ersten Band, alle anderen leer
Ausgabe auf dem ersten Band

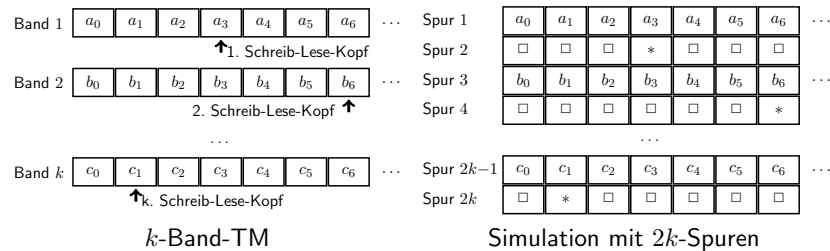
Mehrbandmaschinen (3)

Theorem

Jede Mehrband-TM kann von einer 1-Band TM simuliert werden.

Beweis:

- Sei M eine k -Band-TM. Wenn $k = 1$, dann nichts zu zeigen.
- Für $k > 1$ verwenden wir eine $2 \cdot k$ -Spuren-TM um M zu simulieren.



k -Band-TM

Simulation mit $2k$ -Spuren

Mehrbandmaschinen (4)

- Eingabe $w \in \Sigma^*$ auf dem Eingabeband der Mehrband-Maschine
- 1-Band-Maschine erzeugt Darstellung in $2k$ -Spuren
- 1-Band-Maschine simuliert anschließend Berechnungsschritte.
- Bei Akzeptanz der Mehrband-TM transformiert die 1-Band-TM die Spurendarstellung in die Darstellung der Ausgabe.
- Simulation eines Berechnungsschrittes der Mehrband-TM:
 - 1) lese den verwendeten Bandbereich von links nach rechts
 - 2) speichere alle k Kopfpositionen (durch Zustände)
 - 3) führe Schritt der Mehrband-TM aus, durch Anpassen der Bandinhalte und der Kopfpositionen

□